UNIT – 1 (NETWORKS BASICS)

Computer Network

- A computer network is a system in which multiple computers are connected to each other to share information and resources.
- The physical connection between networked computing devices is established using either cable media or wireless media.
- The best-known computer network is the Internet.

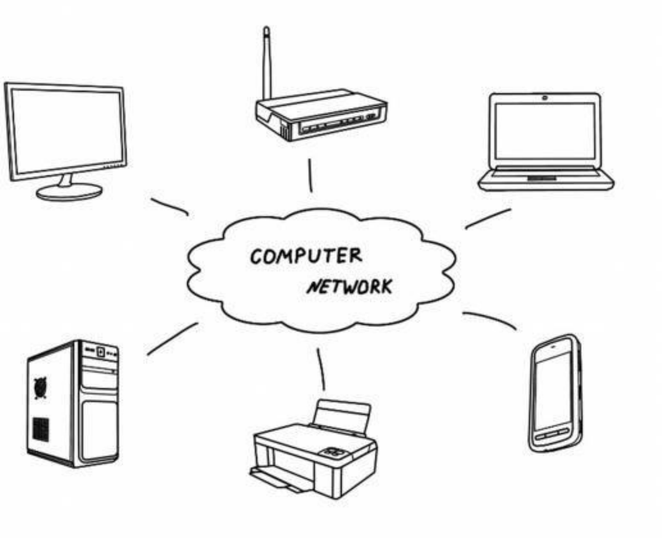


Figure 1: Computer Network

Advantages of Computer Networks

- **File sharing**
  The major advantage of a computer network is that is allows file sharing and remote file access. A person sitting at one workstation that is connected to a network can easily see files present on another workstation, provided he is authorized to do so.
- **Resource sharing**
  All computers in the network can share resources such as printers, fax machines, modems, and scanners.
- **Better connectivity and communications**
  It allows users to connect and communicate with each other easily. Various communication applications included e-mail and groupware are used. Through e-mail, members of a network can send message and ensure safe delivery of data to other members, even in their absence.
- **Internet access**
  Computer networks provide internet service over the entire network. Every single computer attached to the network can experience the high speed internet.
- **Entertainment**
  Many games and other means of entertainment are easily available on the internet. Furthermore, Local Area Networks (LANs) offers and facilitates other ways of enjoyments, such as many players are connected through LAN and play a particular game with each other from remote location.
- **Inexpensive system**

Shared resources mean reduction in hardware costs. Shared files mean reduction in memory requirement, which indirectly means reduction in file storage expenses. A particular software can be installed only once on the server and made available across all connected computers at once. This saves the expense of buying and installing the same software as many times for as many users.

- **Flexible access**
  A user can log on to a computer anywhere on the network and access his files. This offers flexibility to the user as to where he should be during the course of his routine.
- **Instant and multiple access**
  Computer networks are multiply processed .many of users can access the same information at the same time. Immediate commands such as printing commands can be made with the help of computer networks.

Disadvantages of Computer Networks

- **Lack of data security and privacy**
  Because there would be a huge number of people who would be using a computer network to get and share some of their files and resources, a certain user's security would be always at risk. There might even be illegal activities that would occur, which you need to be careful about and aware of.
- **Presence of computer viruses and malwares**
  If even one computer on a network gets affected by a virus, there is a possible threat for the other systems getting affected too. Viruses can spread on a network easily, because of the inter-connectivity of workstations. Moreover, multiple systems with common resources are the perfect breeding ground for viruses that multiply.
- **Lack of Independence**
  Since most networks have a centralized server and dependent clients, the client users lack any freedom whatsoever. Centralized decision making can sometimes hinder how a client user wants to use his own computer.
- **Lack of Robustness**
  As previously stated, if a computer network's main server breaks down, the entire system would become useless. Also, if it has a bridging device or a central linking server that fails, the entire network would also come to a standstill.
- **Need an efficient handler**
  For a computer network to work efficiently and optimally, it requires high technical skills and know-how of its operations and administration. A person just having basic skills cannot do this job. Take note that the responsibility to handle such a system is high, as allotting permissions and passwords can be daunting. Similarly, network configuration and connection is very tedious and cannot be done by an average technician who does not have advanced knowledge.

Use (Applications) of Computer Networks

- **Financial services**
  Nowadays, almost all the financial services depend on the computer network. You can access the financial services across the world. For example, a user can transfer money from one place to another by using the electronic fund transfer feature. You can use networking in various financial areas such as ATM, foreign exchange and credit history search.
- **Business**

Nowadays, most of the works of businesses are done over the computers. To exchange the data and ideas, you need an effective data and resources sharing features. To do this, you need to connect the computer with each other through a network. For example, a person of one department of an organization can share or access the electronic data of other department through network.

- **Email services**
  A computer network provides you the facility to send or receive mails across the globe in few seconds.
- **Mobile applications**
  By using the mobile applications, such as cellular or wireless phones, you can communicate (exchange your views and ideas) with one other.
- **Directory services**
  It provides you the facility to store files on a centralized location to increase the speed of search operation worldwide.
- **Teleconferencing**
  It contains voice conferencing and video conferencing which are based in networking. In teleconferencing the participants need not to be presented at the same location.

Types of Computer Networks

LAN (Local Area Network)

- It is privately-owned networks within a single building or campus of up to a few kilometers in size.
- They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information.
- LANs are easy to design and troubleshoot
- In LAN, all the machines are connected to a single cable.
- Different types of topologies such as Bus, Ring, Star and Tree are used.
- The data transfer rates for LAN is up to 10 Gbits/s.
- They transfer data at high speeds. High transmission rate are possible in LAN because of the short distance between various computer networks.
- They exist in a limited geographical area.

Advantages

- LAN transfers data at high speed.
- LAN technology is generally less expensive.

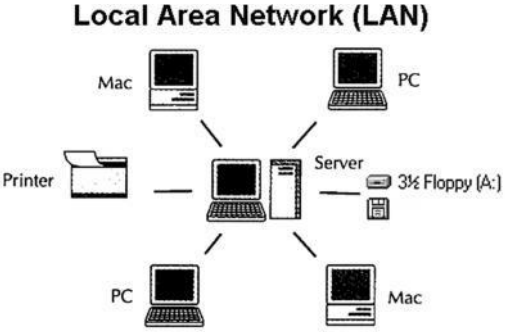


Figure 2: Local Area Network

MAN (Metropolitan Area Network)

- MAN is a larger version of LAN which covers an area that is larger than the covered by LAN but smaller than the area covered by WAN.
- A metropolitan area network or MAN covers a city. The best-known example of a MAN is the cable television network available in many cities.
- MAN connects two or more LANs.
- At first, the companies began jumping into the business, getting contracts from city governments to wire up an entire city.
- The next step was television programming and even entire channels designed for cable only.

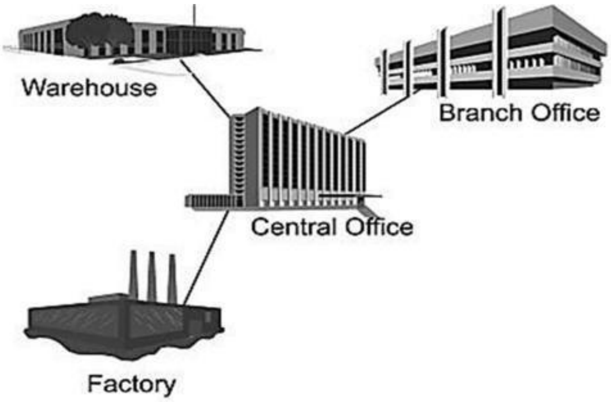


Figure 3: Metropolitan Area Network

WAN (Wide Area Network)

- WAN spans a large geographical area, often a country or region.
- WAN links different metropolitan's countries and national boundaries there by enabling easy communication.
- It may be located entirely within a state or a country or it may be interconnected around the world.
- It contains a collection of machines intended for running user (i.e., application) programs. We will follow traditional usage and call these machines hosts.
- The communication between different users of WAN is established using leased telephone lines or satellite links and similar channels.

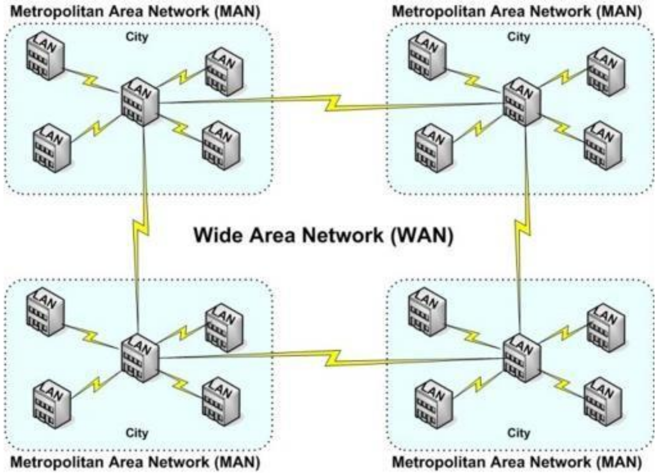

Metropolitan Area Network (MAN)
City
Metropolitan Area Network (MAN)
City
Wide Area Network (WAN)
City
Metropolitan Area Network (MAN)
City
Metropolitan Area Network (MAN)
LAN

Figure 4: Wide Area Network

Difference between LAN, MAN and WAN

Parameter	LAN	MAN	WAN
Area covered	Covers small area. i.e. within building	Covers larger than LAN & smaller than WAN	Covers large area
Error rates	Lowest	Moderate	Highest
Transmission speed	High speed	Moderate speed	Low speed
Equipment cost	Inexpensive	Moderate expensive	Most expensive
Design & maintenance	Easy	Moderate	Difficult

Internet

- The internet is a type of world-wide computer network.
- The internet is the collection of infinite numbers of connected computers that are spread across the world.
- We can also say that, the Internet is a computer network that interconnects hundreds of millions of computing devices throughout the world.
- It is established as the largest network and sometimes called network of network that consists of numerous academic, business and government networks, which together carry various information.
- Internet is a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
- When two computers are connected over the Internet, they can send and receive all kinds of information such as text, graphics, voice, video, and computer programs.

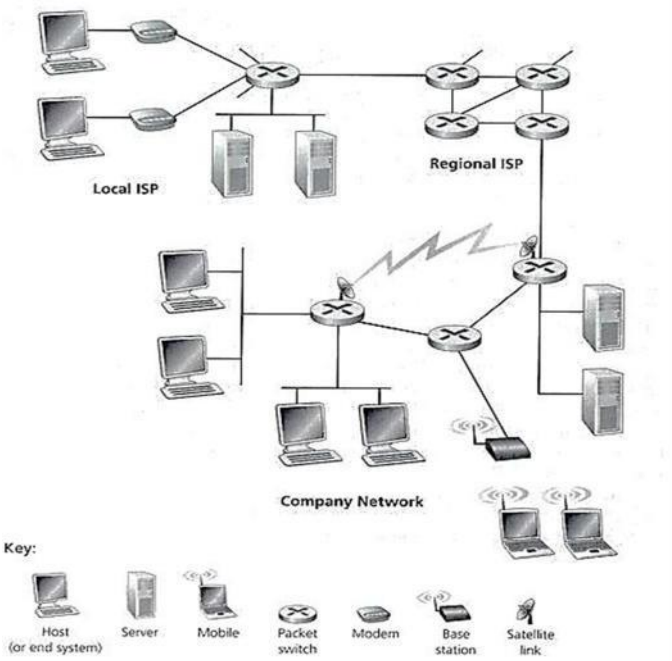


Figure 5: Some pieces of the Internet

Protocol

- A protocol is a set of rules that governs (manages) data communications.
- Protocols defines methods of communication, how to communicate, when to communicate etc.
- A protocol is an agreement between the communicating parties on how communication is to proceed.
- Important elements of protocols are
  1. Syntax 2. Semantics 3. Timing
- **Syntax**:- Syntax means format of data or the structure how it is presented e.g. first eight bits are for sender address, next eight bits are for receiver address and rest of the bits for message data.
- **Semantics**:- Semantics is the meaning of each section of bits e.g. the address bit means the route of transmission or final destination of message.
- **Timing**:- Timing means, at what time data can be sent and how fast data can be sent.
- Some protocols also support message acknowledgement and data compression designed for reliable and/or high-performance network communication.
- Example: HTTP, IP, FTP etc…

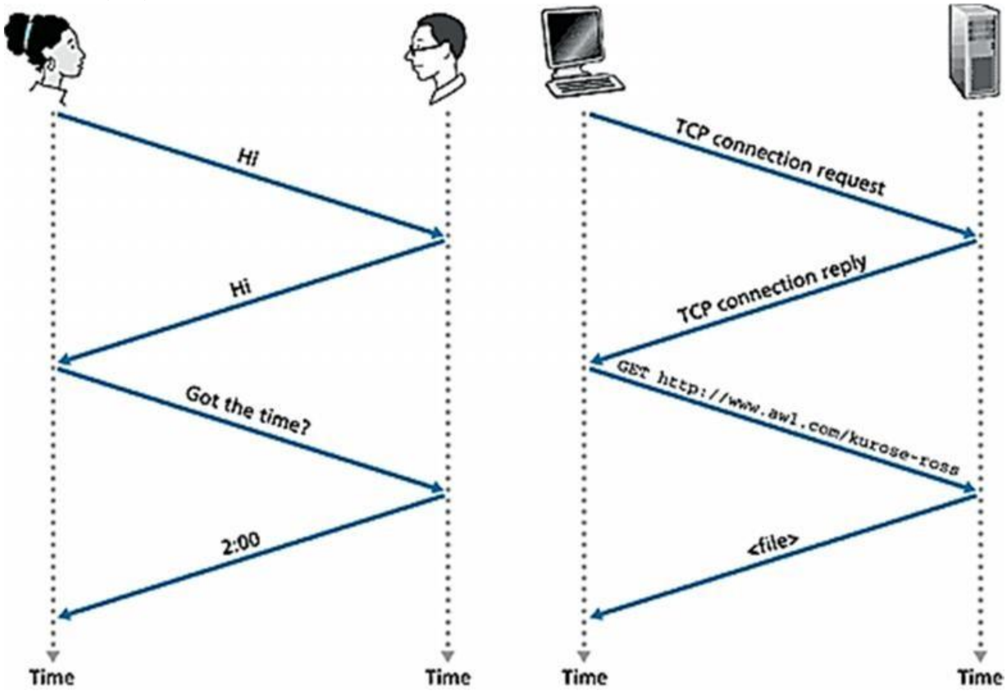


Figure 6: A human protocol and a computer network protocol

The Network Edge

- It defines those computers of the network used at the edge (end) of the network. These computers are known as hosts or end system.
- Host can be classified into the following two types:
  - **Clients**: Refer to the computer systems that request servers for the completion of a task. The clients are generally called desktop PCs or workstations.

- ➢ **Servers**: Refer to the computer systems that receive requests from the clients and process them. After the processing is complete, the servers send a reply to the clients who sent the request.

- The concept of clients and servers is essential in the network design. The various networks design models are as follows:
  1. Peer to Peer network 2. Client Server network

Peer to Peer network

- In this network group of computers is connected together so that users can share resources and information.
- There is no central location (server) for authenticating users, storing files, or accessing resources and each of them works as both client and server.
- This means that users must remember which computers in the workgroup have the shared resource or information that they want to access.
- **Advantage**:
  - ➢ It is easy to setup.
  - ➢ There is no need of any committed server as each peer acts as both server and client.
  - ➢ The network implementation is quite cheap.
  - ➢ The resources of a peer can be shared with other peers very easily in the network.
- **Disadvantage:**
  - ➢ The speed of the network decreases due to heavy usage.
  - ➢ It is not easy to keep track of information on each computer.
  - ➢ There is no central backup of files and folders.
  - ➢ Network and data security are weak.

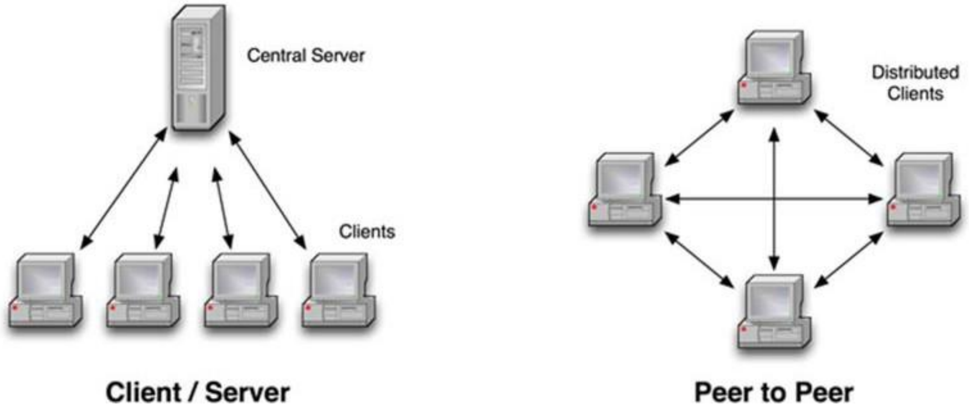


Figure 7: Network Edge - Client/Server Network and Peer to Peer

Client/Server network

- A client/server network is a system where one or more computers called clients connect to a central computer named as server to share or use resources.
  - The client requests a service from server, which may include running an application, querying database, printing a document, performing a backup or recovery procedure. The request made by the client is handled by server.
  - A client/server network is that in which the files and resources are centralized. This means that the server can hold them and other computers (Client) can access them.

- **Advantage**:
    - ➢ The server system holds the shared files.
    - ➢ The server system can be scheduled to take the file backups automatically.
    - ➢ Network access is provided only to authorize users through user security at the server.
    - ➢ The server system is a kind of central repository for sharing printer with clients.
    - ➢ Internet access, e-mail routing and such other networking tasks are quite easily managed by the server.
    - ➢ The software applications shared by the server are accessible to the clients.
- **Disadvantage:**
    - ➢ The implementation of the network is quite expensive.
    - ➢ An NOS (Network Operating System) is essential.
    - ➢ If server fails, the entire network crashes.
    - ➢ There may be congestion if more than one client requests for a service at the same time.

Techniques used in data communications to transfer data

1. Connection-oriented method 2. Connectionless method

Connection-oriented method

- Connection-oriented communication includes the steps of setting up a call from one computer to another, transmitting/receiving data, and then releasing the call, just like a voice phone call.
- However, the network connecting the computers is a packet switched network, unlike the phone system's circuit switched network.
- Connection-oriented communication is done in one of two ways over a packet switched network:
    1. Without virtual circuits
    2. With virtual circuits.

Without virtual circuits:

- This is what TCP does in the Internet.
- The only two machines in the Internet are aware about connection which is established between the two computers at the endpoints.
- The Internet itself, its routers and links have no information about the presence of a connection between the two computers.
- This means that all of the packets flowing between the two computers can follow different routes.
- One benefit of establishing the connection is that the flow of packets from the source to the destination can be slowed down if the Internet is congested and speeded up when congestion disappears.
- Another benefit is that the endpoints can anticipate traffic between them, and agree to cooperate to ensure the integrity and continuity of the data transfers. This allows the network to be treated as a "stream" of data.

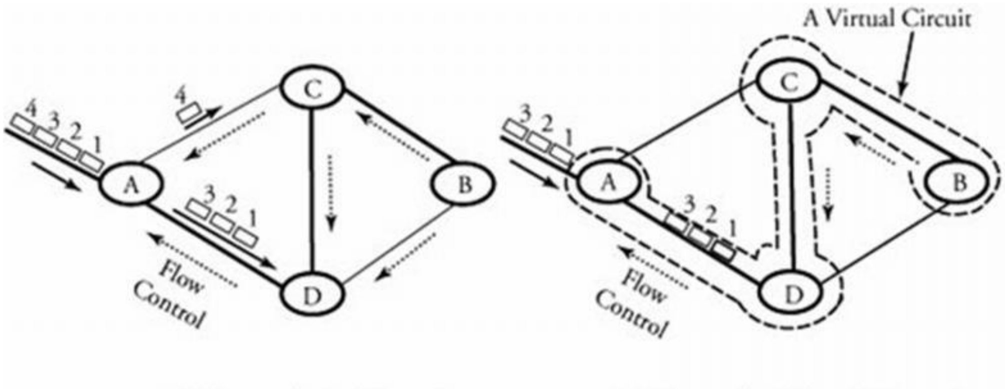
With virtual circuit:

- This is not used in the Internet, but is used in other types of networks (eg. the "X.25" protocol, still popular in Europe).

- The routers within the network route all packets in one connection over the same route. The advantage is that video and voice traffic are easier to carry, because routers can reserve memory space to buffer the transmission.

Connectionless method

- Connectionless communication is just packet switching where no call establishment and release occur.
- A message is broken into packets, and each packet is transferred separately. Moreover, the packets can travel different route to the destination since there is no connection.
- Connectionless service is typically provided by the UDP (User Datagram Protocol). The packets transferred using UDP are also called datagrams.



(a) Connectionless Network

(b) Connection-Oriented Network

Feature	Connectionless	Connection-oriented
How is data sent?	one packet at a time	as continuous stream of packets
Do packets follow same route?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in network?	no	virtual circuit: yes without virtual circuit: no
Are resources reserved in communicating hosts?	no	yes
Is connection establishment done?	no	yes
Is state information stored at network nodes?	no	virtual circuit: yes without virtual circuit: no
What is impact of node/switch crash?	only packets at node are lost	all virtual circuits through node fail
What addressing information is needed on each packet?	full source and destination address	virtual circuit: a virtual circuit number without virtual circuit: full source and destination address

Transmission Media

- A transmission media can be defined as anything that can carry information from a source to a destination.
- On the basis of transmission of data, the transmission media can be classified in to two categories:
    1. Guided (Physical) transmission media
    2. Unguided (Wireless) transmission media

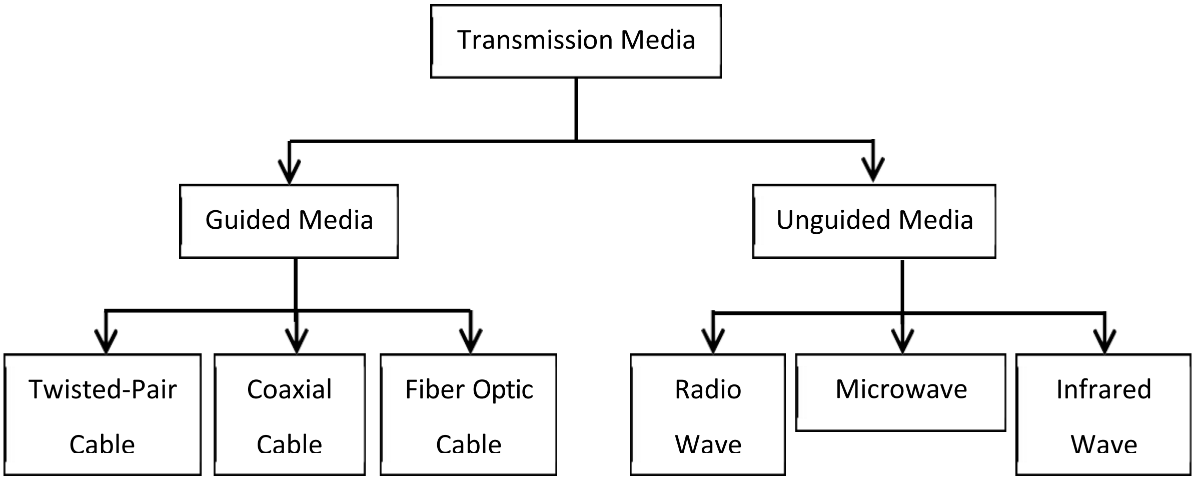


Figure 8: Classification Transmission Media

Guided Transmission Media

- Guided media are those that provide a channel from one device to another.
- The three Guided (Physical) media commonly used for data transmission are:
    1. Twisted-Pair 2. Coaxial 3. Fiber Optics

1. Twisted Pair

- A twisted pair consists of two insulated copper wires, typically about 1 mm thick.
- The wires are twisted together in a helical form, just like a DNA molecule.
- Twisting is done because two parallel wires constitute a fine antenna.
- When the wires are twisted, the waves from different twists cancel out, so the wire radiates less effectively.

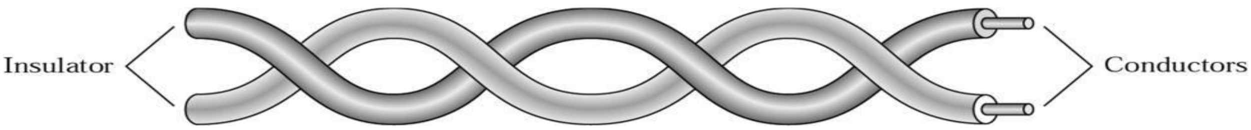


Figure 9: Twisted Pair Cable

Why Cable is twisted?

- If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relatives to the noise or crosstalk sources.
- This results in a difference at the receiver.
- By twisting the pair, a balance is maintained.

Types of Twisted-Pair Cable

1) Unshielded twisted-pair (UTP)

- Twisted pair cabling comes in several varieties, two of which are important for computer networks.
- **Category 3** twisted pairs consist of two insulated wires gently twisted together.
- Most office buildings had one category 3 cable running from a central wiring closet on each floor into each office.
- **Category 5** is the more advanced twisted pairs were introduced.
- They are similar to category 3 pairs, but with more twists per centimetre, which results in less crosstalk and a better-quality signal over longer distances, making them more suitable for high-speed computer communication.
- Up-and-coming categories are 6 and 7, which are capable of handling signals with bandwidths of 250 MHz and 600 MHz, respectively (versus a mere 16 MHz and 100 MHz for categories 3 and 5 respectively).

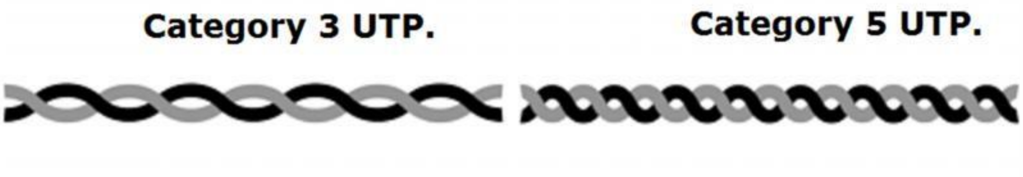


Figure 10: Unshielded twisted-pair

2) Shielded twisted-pair (STP)

- STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors.
- Metal casing improves the quality of cable by preventing the penetration of noise or crosstalk.
- It is bulkier and more expensive.
- **Applications:**
  - Used in telephone lines to provide voice and data channels.
  - The DSL lines uses by telephone companies use the high-bandwidth capability of UTP cables.
  - LANs, such as 10Base-T, 100Base-T also uses twisted-pair cables.

2. Coaxial Cable

- It has better shielding than twisted pairs, so it can span longer distances at higher speeds.
- Two kinds of coaxial cable are widely used. One kind is 50-ohm cable which is commonly used when it is intended for digital transmission from the start.
- The other kind is 75-ohm cable which is commonly used for analog transmission and cable television but is becoming more important with the advent of Internet over cable.
- A coaxial cable consists of a stiff copper wire as the core surrounded by an insulating material.
- The insulator is encased by a cylindrical conductor, often as a closely-woven braided mesh.
- The outer conductor is covered in a protective plastic sheath.
- The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.
- The bandwidth possible depends on the cable quality, length and signal-to-noise ratio of the data signal. Modern cables have a bandwidth of close to 1 GHz.

- Coaxial cables used is widely used within the telephone system for long-distance lines but have now largely been replaced by fiber optics on long-haul routes.

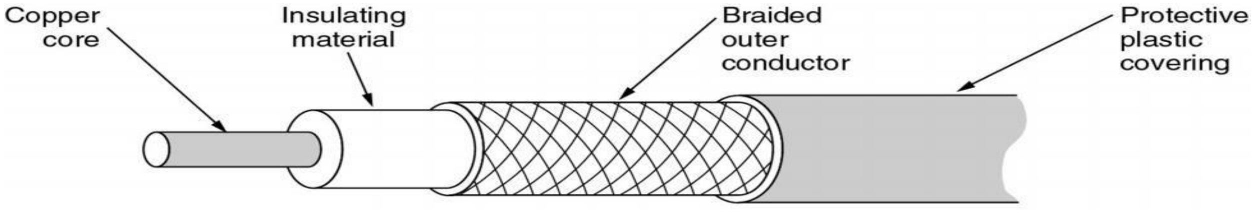


Figure 11: Coaxial Cable

3. Fiber Optics

- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through a core is reflected off the cladding instead of being refracted into it.

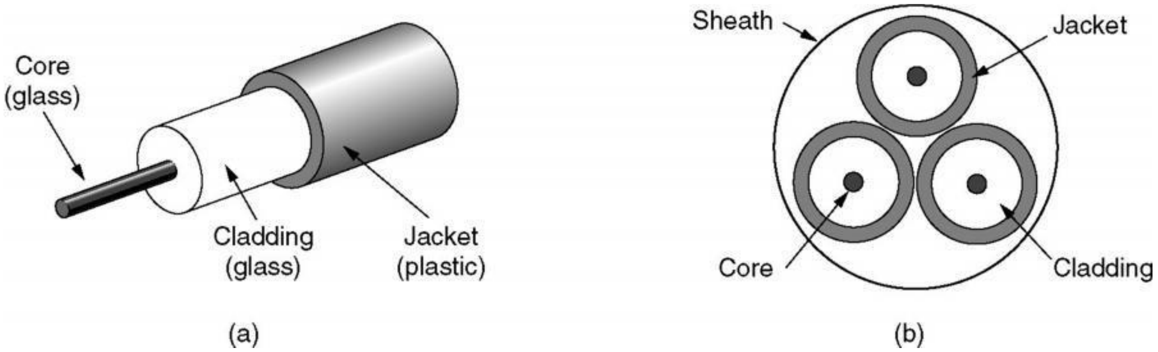


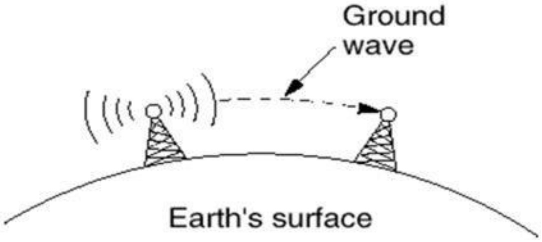
Figure 12: Fiber Optic Cable

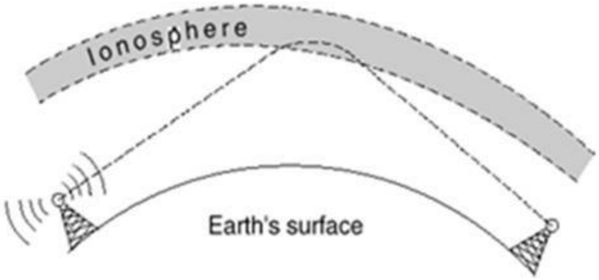
- Fiber optic cables are similar to coax, except without the braid.
- Figure shows a single fiber viewed from the side. At the centre is the glass core through which the light propagates.
- The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all the light in the core.
- Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped in bundles, protected by an outer sheath. Figure shows a sheath with three fibers.

Unguided (Wireless) transmission media

- Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication.
  1. Radio Transmission
  2. Infra Red
  3. Micro Wave Transmission
  4. Light Wave Transmission

1. **Radio Transmission**
    - Radio waves are easy to generate, can travel long distances, and can penetrate buildings easily, so they are widely used for communication, both indoors and outdoors.
    - Radio waves also are omnidirectional, meaning that they travel in all directions from the source, so the transmitter and receiver do not have to be carefully aligned physically.
    - The properties of radio waves are frequency dependent.
    - At low frequencies, radio waves pass through obstacles well, but the power falls off sharply with distance from the source, roughly as $1/r^2$ in air.
    - At high frequencies, radio waves tend to travel in straight lines and bounce off obstacles. They are also absorbed by rain.
    - At all frequencies, radio waves are subject to interference from motors and other electrical equipment.





- In the VLF, LF, and MF bands, radio waves follow the curvature of the earth.
- In the HF they bounce off the ionosphere

2. **Microwave Transmission**
    - Since the microwaves travel in a straight line, if the towers are too far apart, the earth will get in the way. Consequently, repeaters are needed periodically.
    - Unlike radio waves at lower frequencies, microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space.
    - Above 100 MHz, the waves **travel in straight lines** and can therefore be narrowly focused. Concentrating all the energy into a small beam using a **parabolic antenna** gives a much higher signal to noise ratio.
    - **Advantages:**
        - No right way is needed (compared to wired media).
        - Relatively inexpensive.
        - Simple to install.
    - **Disadvantages:**
        - Do not pass through buildings well.
        - Multipath fading problem (the delayed waves cancel the signal).
        - Absorption by rain above 8 GHz.
        - Severe shortage of spectrum.
3. **Infrared**
    - Unguided infrared and millimeter waves are widely used for short-range communication.
    - The remote controls used on televisions, VCRs, and stereos all use infrared communication.

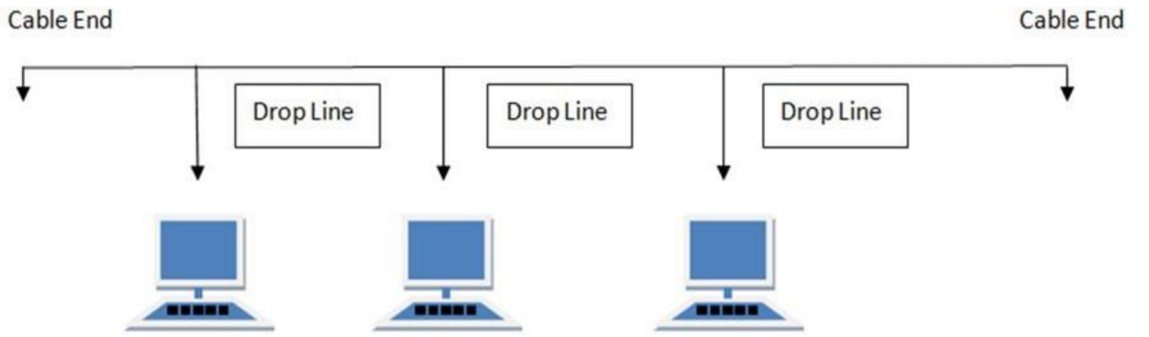
- They are relatively directional, cheap, and easy to build but have a major drawback: they do not pass through solid objects (try standing between your remote control and your television and see if it still works).
- In general, as we go from long-wave radio toward visible light, the waves behave more and more like light and less and less like radio.
- On the other hand, the fact that infrared waves do not pass through solid walls well is also a plus.
- It means that an infrared system in one room of a building will not interfere with a similar system in adjacent rooms or buildings.
- Furthermore, security of infrared systems against eavesdropping is better than that of radio systems precisely for this reason.
- Therefore, no government license is needed to operate an infrared system, in contrast to radio systems, which must be licensed outside the ISM bands.

Topologies (Network Topologies)

- Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.
- A Network Topology is the arrangement with which computer systems or network devices are connected to each other.
- Types of network topologies :
  1. Bus
  2. Star
  3. Tree
  4. Ring
  5. Mesh
  6. Hybrid

Bus Topology

- Bus topology is a network type in which every computer and network device is connected to single cable.



Features:

- It transmits data only in one direction.
- Every device is connected to a single cable.

Advantages:

- It is cost effective (cheaper).
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand.

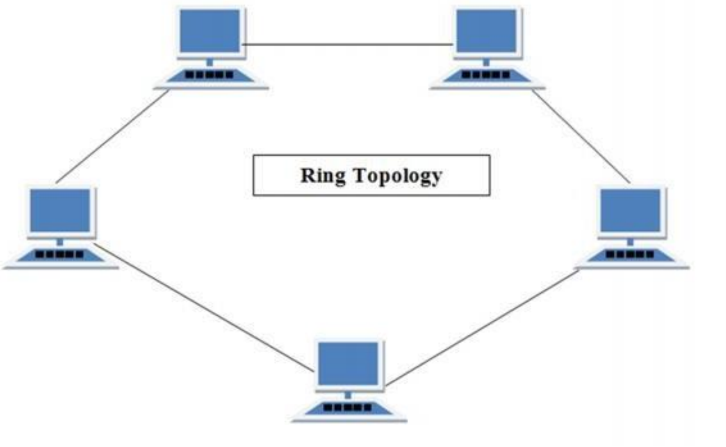
- Easy to expand joining two cables together.

Disadvantages:

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.

Ring Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.



Features:

- A number of repeaters are used and the transmission is unidirectional.
- Date is transferred in a sequential manner that is bit by bit.

Advantages:

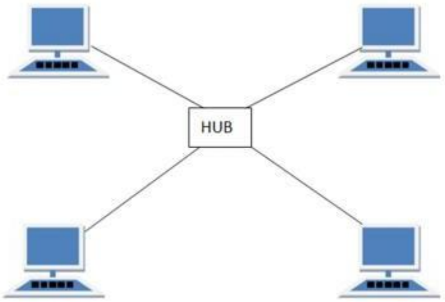
- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand.

Disadvantages:

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

Star Topology

- In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features:

- Every node has its own dedicated connection to the hub.
- Acts as a repeater for data flow.
- Can be used with twisted pair, Optical Fiber or coaxial cable.

Advantages:

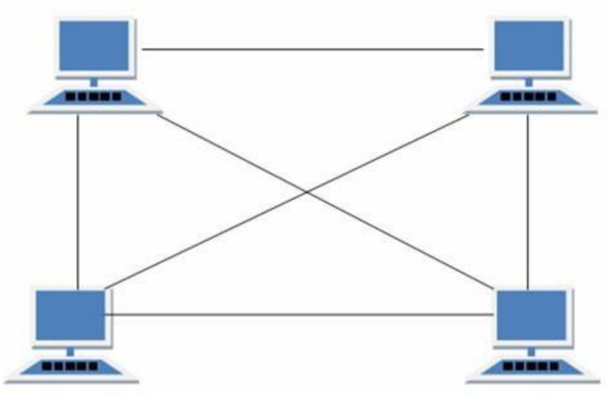
- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot.
- Easy to setup and modify.
- Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantages:

- Cost of installation is high.
- Expensive to use.
- If the hub is affected then the whole network is stopped because all the nodes depend on the hub.

Mesh Topology

- It is a point-to-point connection to other nodes or devices.
- Traffic is carried only between two devices or nodes to which it is connected.



Features:

- Fully connected.
- Robust.
- Not flexible.

Advantages:

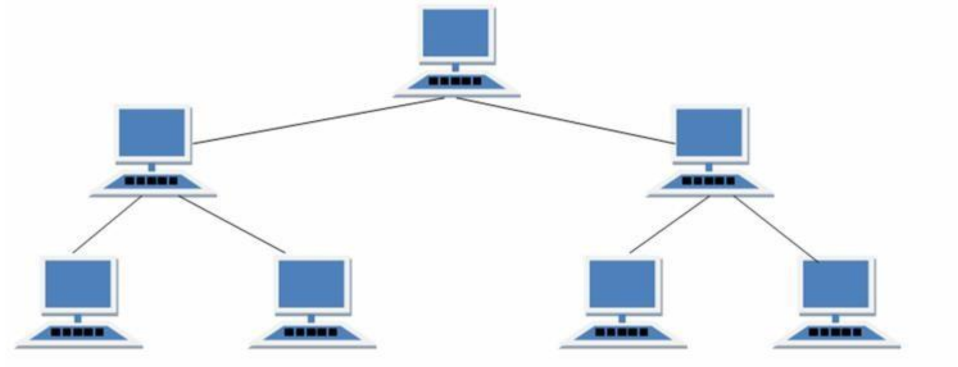
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages:

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

Tree Topology

- It has a root node and all other nodes are connected to it forming a hierarchy.
- It is also called hierarchical topology.
- It should at least have three levels to the hierarchy.



Features:

- Ideal if workstations are located in groups.
- Used in Wide Area Network.

Advantages:

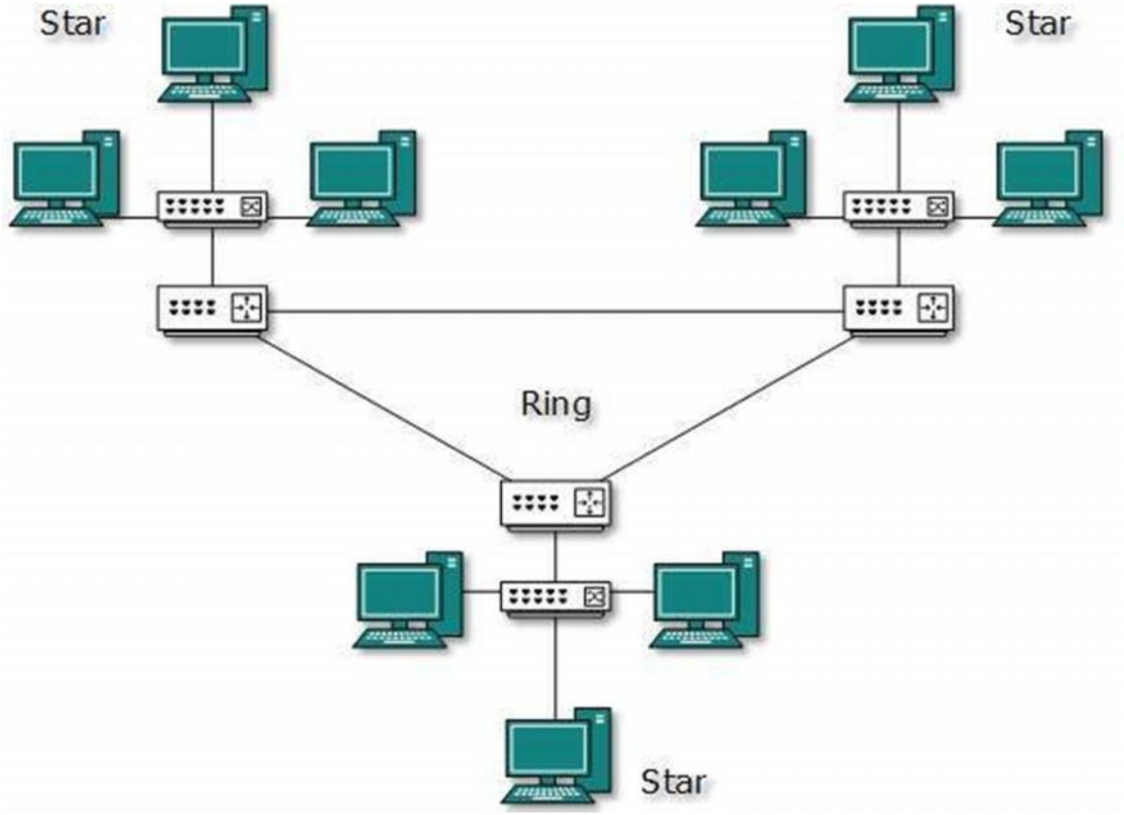
- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages:

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails then network fails.

Hybrid Topology

- A network structure whose design contains more than one topology is said to be hybrid topology.
- For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features:

- It is a combination of two or more topologies
- Inherits the advantages and disadvantages of the topologies included

Advantages:

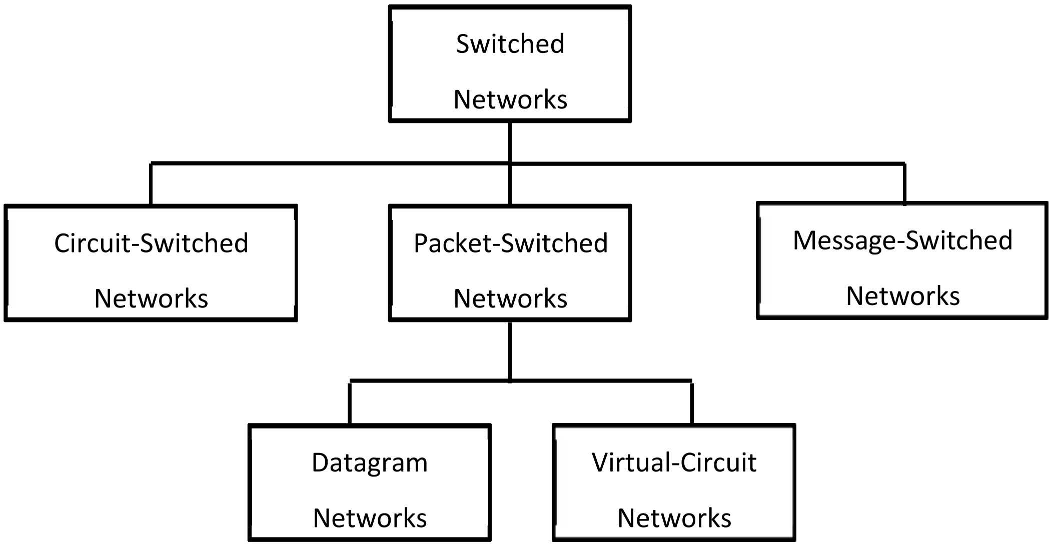
- Reliable as error detecting and trouble shooting is easy.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages:

- Complex in design.
- Costly.

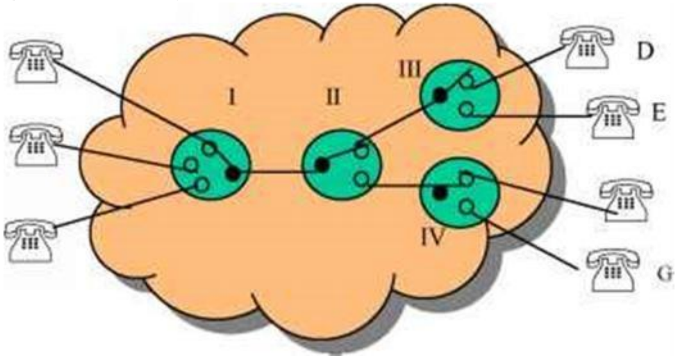
The Network Core

- Network core defines the connection of different network segments together and the process to transmit the data packets across the network.
- The network core is implemented through the use of switching techniques.
- The classification of switching network is shown below:

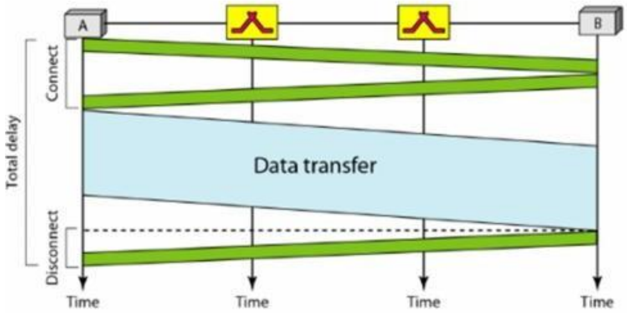


Circuit Switching

- Circuit switching is used in public telephone networks and is the basis for private networks built on leased-lines.
- Circuit switching was developed to handle voice traffic but also digital data (although inefficient)
- With circuit switching a dedicated path is established between two stations for communication.



- Switching and transmission resources within the network are reserved for the exclusive use of the circuit for the duration of the connection.
- The connection is transparent: once it is established, it appears to attach devices as if there were a direct connection.
- Communication via circuit switching involves three phases:
    1. Circuit Establishment
    2. Data Transfer
    3. Circuit Disconnect



- Connection path must be established before data transmission begins. Nodes must have switching capacity and channel capacity to establish connection.
- Circuit switching is inefficient
    1. Channel capacity dedicated for duration of connection
    2. If no data, capacity wasted
- Set up (connection) takes time
- Once connected, transfer is transparent to the users
    1. Data is transmitted at a fixed data rate with no delay (except for the propagation delay)
- Developed for voice traffic (phone)
    1. May also be used for data traffic via modem
- Interconnection of telephones within a building or office.
- In circuit switching, a direct physical connection between two devices is created by space-division switches, time-division switches, or both OR Circuit switching use any of below two technologies:

Space Division Switching

- Developed for analog environment.
- In a space-division switch, the path from one device to another is spatially separate from other paths.
- A crossbar is the most common space-division switch. It connects n inputs to m outputs via n × m cross points.
- Crossbar switch.

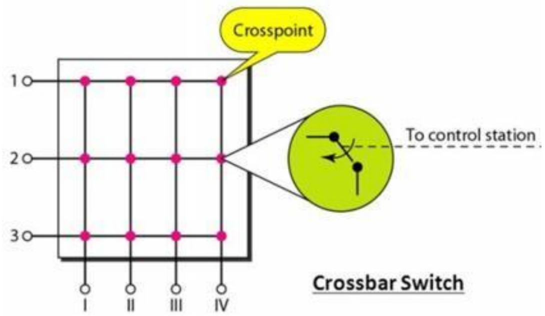
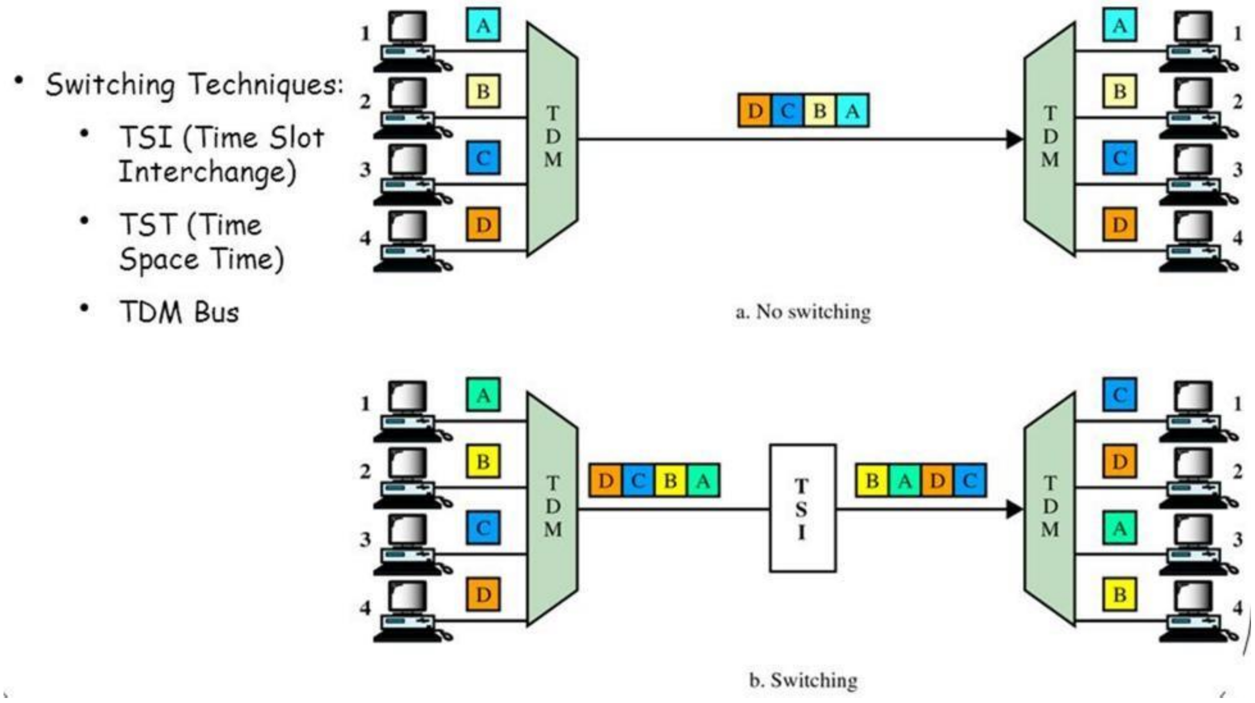


Figure 13: Space Division Switching

Time Division Switching

- In a time-division switch, the inputs are divided in time, using TDM. A control unit sends the input to the correct output device.
- Use digital time division techniques to set up and maintain virtual circuits.



- Switching Techniques:
  - TSI (Time Slot Interchange)
  - TST (Time Space Time)
  - TDM Bus

a. No switching

b. Switching

Packet Switching

- Packet switching was designed to provide a more efficient facility than circuit-switching for bursty data traffic.
- With packet switching, a station transmits data in small blocks, called packets.
- At each node packets are received, stored briefly (buffered) and passed on to the next node.
  1. Store and forward mechanism
- Each packet contains some portion of the user data plus control info needed for proper functioning of the network.
- A key element of packet-switching networks is whether the internal operation is datagram or virtual circuit (VC).
  1. With internal VCs, a route is defined between two endpoints and all packets for that VC follow the same route.
  2. With internal diagrams, each packet is treated independently, and packets intended for the same destination may follow different routes.
- Examples of packet switching networks are X.25, Frame Relay, ATM and IP.
- Station breaks long message into packets. Packets sent one at a time to the network.
- Packets handled in two ways:

  1. **Datagram**
     - Each packet treated independently
     - Packets can take any practical route
     - Packets may arrive out of order
     - Packets may go missing
     - Up to receiver to re-order packets and recover from missing packets

2. **Virtual Circuit**
    - Preplanned route established before any packets sent.
    - Once route is established, all the packets between the two communicating parties follow the same route through the network
    - Call request and call accept packets establish connection (handshake)
    - Each packet contains a Virtual Circuit Identifier (VCI) instead of destination address
    - No routing decisions required for each packet
    - Clear request to drop circuit
    - Not a dedicated path

Message Switching

- This technique was somewhere in middle of circuit switching and packet switching.
- In message switching, the whole message is treated as a data unit and is transferred in its entirety.
- A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop.
- If the next hop is not having enough resource to accommodate large size message, the message is stored and switch waits.

UNIT – 2 (NETWORKING MODELS)

OSI Layer Architecture

- OSI model is based on a proposal developed by the International Standards Organization (ISO) as a first step toward international standardization of the protocols used in the various layers.
- It was revised in 1995.
- The model is called the OSI (Open Systems Interconnection) Reference Model because it deals with connecting open systems—that is, systems that are open for communication with other systems.
- The OSI model has seven layers.
    1. Physical Layer
    2. Data Link Layer
    3. Network Layer
    4. Transport Layer
    5. Session Layer
    6. Presentation Layer
    7. Application Layer

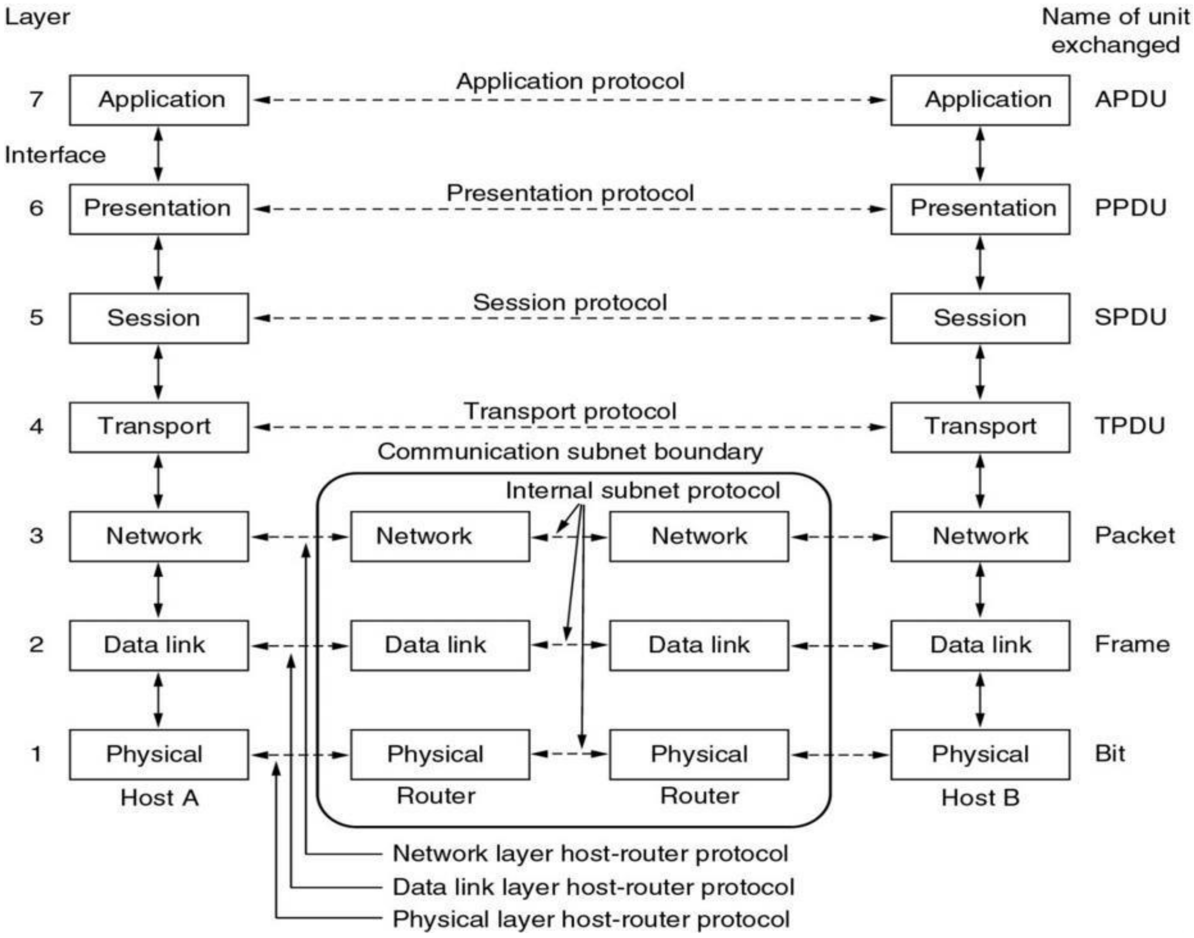


Figure 15: OSI Reference Model

Physical Layer

- The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium.
- It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:
- **Data encoding**: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization.
- **Transmission technique**: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- **Physical medium transmission**: transmits bits as electrical or optical signals appropriate for the physical medium.

Data Link Layer

- The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link.
- To do this, the data link layer provides:
- **Link establishment and termination**: establishes and terminates the logical link between two nodes.
- **Frame traffic control**: tells the transmitting node to "back-off" (stop) when no frame buffers are available.
- **Frame sequencing**: transmits/receives frames sequentially.
- **Frame acknowledgment**: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non-acknowledged frames and handling duplicate frame receipt.
- **Frame delimiting**: creates and recognizes frame boundaries.
- **Frame error checking**: checks received frames for integrity.
- **Media access management**: determines when the node "has the right" to use the physical medium.

Network Layer

- The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors.
- To do this, the data link layer provides:
- **Routing**: routes frames among networks.
- **Subnet traffic control**: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- **Frame fragmentation**: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- **Logical-physical address mapping**: translates logical addresses or names, into physical addresses.
- **Subnet usage accounting**: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Transport Layer

- The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves (release) the higher layer protocols from any concern with the transfer of data between them and their peers.

- The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.
- The transport layer provides:
- **Message segmentation**: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- **Message acknowledgment**: provides reliable end-to-end message delivery with acknowledgments.
- **Message traffic control**: tells the transmitting station to "back-off" when no message buffers are available.
- Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.
- The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries.
- In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

Session Layer

- The session layer allows session establishment between processes running on different stations. It provides:
- **Session establishment, maintenance and termination**: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- **Session support**: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Presentation Layer

- The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, and then translate the common format to a format known to the application layer at the receiving station.
- The presentation layer provides:
- **Character code translation**: for example, ASCII to EBCDIC.
- **Data conversion**: bit order, CR-CR/LF, integer-floating point, and so on.
- **Data compression**: reduces the number of bits that need to be transmitted on the network.
- **Data encryption**: encrypt data for security purposes. For example, password encryption.

Application Layer

- The application layer serves as the window for users and application processes to access network services.
- This layer contains a variety of commonly needed functions:
  1. Resource sharing and device redirection
  2. Remote file access
  3. Remote printer access

4. Inter-process communication
5. Network management
6. Directory services
7. Electronic messaging (such as mail)
8. Network virtual terminals

TCP/IP Reference Model (Internet Protocol Stack Layers)

- Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide.
- TCP/IP either combines several OSI layers into a single layer, or does not use certain layers at all.
- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.
- The TCP/IP model has five layers.
    1. Application Layer
    2. Transport Layer
    3. Internet Layer
    4. Data Link Layer
    5. Physical Network

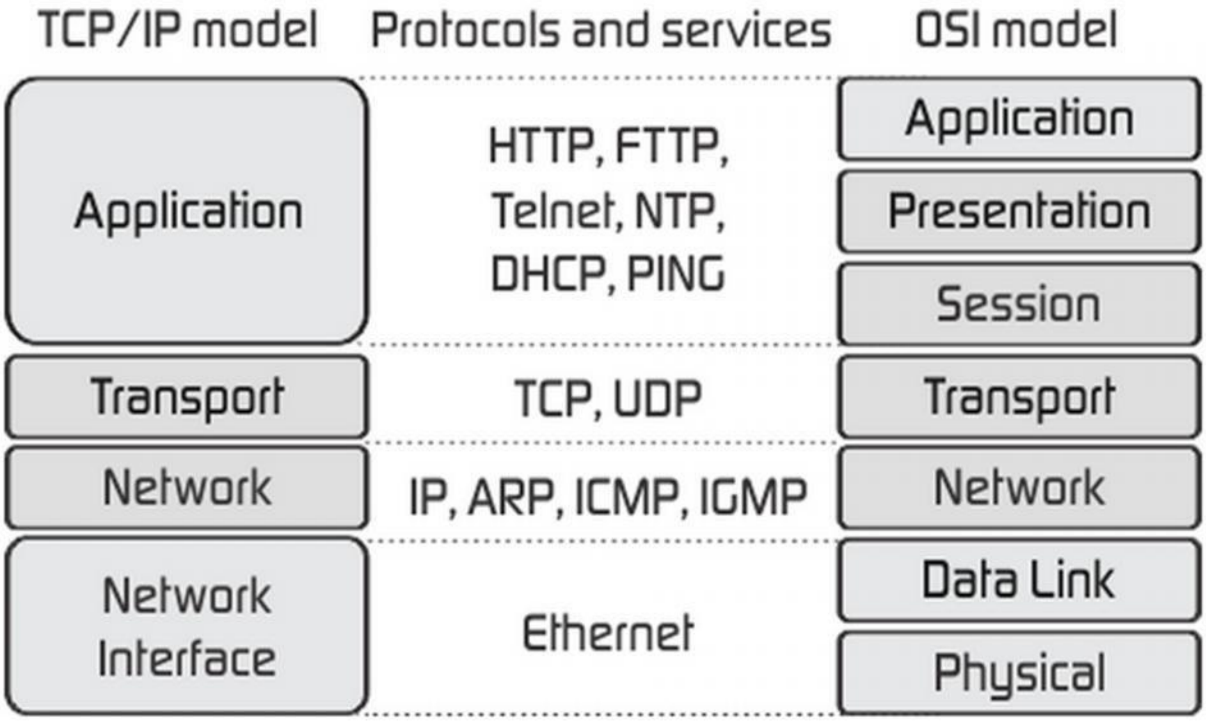


Figure 16: TCP/IP Reference Model

- As we can see from the above figure, presentation and session layers are not there in TCP/IP model. Also note that the Network Access Layer in TCP/IP model combines the functions of Data link Layer and Physical Layer.

Application Layer

- Application layer is the top most layer of four layer TCP/IP model.
- Application layer is present on the top of the Transport layer.
- Application layer defines TCP/IP application protocols and how host programs interface with Transport layer services to use the network.
- Application layer includes all the higher-level protocols like DNS (Domain Naming System), HTTP (Hypertext Transfer Protocol), Telnet, SSH, FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), SMTP (Simple Mail Transfer Protocol), DHCP (Dynamic Host Configuration Protocol), X Windows, RDP (Remote Desktop Protocol) etc.

Transport Layer

- The purpose of Transport layer is to permit devices on the source and destination hosts to carry on a conversation.
- Transport layer defines the level of service and status of the connection used when transporting data.
- The transport layer provides the end-to-end data transfer by delivering data from an application to its remote peer.
- The most-used transport layer protocol is the Transmission Control Protocol (TCP), which provides:
    - Reliable Delivery Data
    - Congestion Control
    - Duplicate Data Suppression
    - Flow Control
- Another transport layer protocol is the User Datagram Protocol (UDP), which provides:
    - Connectionless
    - Best-effort service
    - Unreliable
- UDP is used by applications that need a fast transport mechanism and can tolerate the loss of some data.

Network Layer (Internet Layer)

- The internet layer also called the network layer.
- Internet layer pack data into data packets known as IP datagrams, which contain source and destination address (logical address or IP address) information that is used to forward the datagrams between hosts and across networks.
- The Internet layer is also responsible for routing of IP datagrams.
- Internet Protocol (IP) is the most important protocol in this layer.
- It is a connectionless protocol that does not assume reliability from lower layers. IP does not provide reliability, flow control or error recovery.
- IP provides a routing function that attempts to deliver transmitted messages to their destination.
- These message units in an IP network are called an IP datagram.
- Example: IP, ICMP, IGMP, ARP, and RARP.

Network Interface Layer (Network Access Layer)

- Network Access Layer defines details of how data is physically sent through the network, including how bits are electrically or optically signalled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted pair copper wire.
- The protocols included in Network Access Layer are Ethernet, Token Ring, FDDI, X.25, Frame

Relay etc.

OSI(Open System Interconnection)	TCP/IP (Transmission Control Protocol/ Internet Protocol)
OSI provides layer functioning and also defines Functions of all the layers.	TCP/IP model is more based on protocols and Protocols are not flexible with other layers.
In OSI model the transport layer guarantees the delivery of packets	In TCP/IP model the transport layer does not Guarantees delivery of packets.
Follows horizontal approach	Follows vertical approach.
OSI model has a separate presentation layer	TCP/IP doesn’t have a separate presentation layer
OSI is a general model.	TCP/IP model cannot be used in any other
	Application.
Network layer of OSI model provide both Connection oriented and connectionless service.	The Network layer in TCP/IP model provides Connectionless service.
OSI model has a problem of fitting the protocols in the model	TCP/IP model does not fit any protocol
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	In TCP/IP it is not clearly separated its services, interfaces and protocols.
It has 7 layers	It has 4 layers

UNIT – 3 (TCP/IP ADDRESSING)

Concept of Physical and Logical Addressing

Address uniquely identifies a location in the memory. We have two types of addresses that are logical address and physical address. The logical address is a virtual address and can be viewed by the user. The user can’t view the physical address directly. The logical address is used like a reference, to access the physical address.

The fundamental difference between logical and physical address is that **logical address** is generated by CPU during a program execution whereas, the **physical address** refers to a location in the memory unit.
There are some other differences between the logical and physical address. Let us discuss them with the help of comparison chart shown below.

Basis for Comparison	Logical Address	Physical Address
Basic	It is the virtual address generated by CPU	The physical address is a location in a memory unit.
Address Space	Set of all logical addresses generated by CPU in reference to a program is referred as Logical Address Space.	Set of all physical addresses mapped to the corresponding logical addresses is referred as Physical Address.
Visibility	The user can view the logical address of a program.	The user can never view physical address of program
Access	The user uses the logical address to access the physical address.	The user can not directly access physical address.
Generation	The Logical Address is generated by the CPU	Physical Address is Computed by MMU

Definition of Logical Address

Address generated by **CPU** while a program is running is referred as **Logical Address**. The logical address is virtual as it does not exist physically. Hence, it is also called as **Virtual Address**. This address is used as a reference to access the physical memory location. The set of all logical addresses generated by a programs perspective is called **Logical Address Space**.
The logical address is mapped to its corresponding physical address by a hardware device called **Memory-Management Unit**. The address-binding method used by MMU generates **identical** logical and physical address during **compile time** and **load time**. However, while **run-time** the address-binding methods generate **different** logical and physical address.

Definition of Physical Address

Physical Address identifies a physical location in a memory. MMU (**Memory-Management Unit)** computes the physical address for the corresponding logical address. MMU also uses logical address computing physical address. The user never deals with the physical address. Instead, the physical address is accessed by its corresponding logical address by the user.

The user program generates the logical address and thinks that the program is running in this logical address. But the program needs physical memory for its execution. Hence, the logical address must be mapped to the physical address before they are used.

The logical address is mapped to the physical address using a hardware called **Memory-Management Unit**. The set of all physical addresses corresponding to the logical addresses in a Logical address space is called **Physical Address Space.**

Key Differences between Logical and Physical Address in OS

1. The basic difference between Logical and physical address is that Logical address is generated by CPU in perspective of a program. On the other hand, the physical address is a location that exists in the memory unit.
2. The set of all logical addresses generated by CPU for a program is called Logical Address Space. However, the set of all physical address mapped to corresponding logical addresses is referred as Physical Address Space.
3. The logical address is also called virtual address as the logical address does not exist physically in the memory unit. The physical address is a location in the memory unit that can be accessed physically.
4. Identical logical address and physical address are generated by Compile-time and Load time address binding methods.
5. The logical and physical address generated while run-time address binding method differs from each other.
6. The logical address is generated by the CPU while program is running whereas; the physical address is computed by the MMU (Memory Management Unit).

IPV4 Overview

What is Network?

A Network in the world of computers is said to be a collection of interconnected hosts, via some shared media which can be wired or wireless. A computer network enables its hosts to share and exchange data and information over the media. Network can be a Local Area Network spanned across an office or Metro Area Network spanned across a city or Wide Area Network which can be spanned across cities and provinces.

A computer network can be as simple as two PCs connected together via a single copper cable or it can be grown up to the complexity where every computer in this world is connected to every other, called the Internet. A network then includes more and more components to reach its ultimate goal of data exchange. Below is a brief description of the components involved in computer network −

- **Hosts** − Hosts are said to be situated at ultimate end of the network, i.e. a host is a source of information and another host will be the destination. Information flows end to end between hosts. A host can be a user’s PC, an internet Server, a database server etc.
- **Media** − If wired, then it can be copper cable, fiber optic cable, and coaxial cable. If wireless, it can be free-to-air radio frequency or some special wireless band. Wireless frequencies can be used to interconnect remote sites too.
- **Hub** − A hub is a multiport repeater and it is used to connect hosts in a LAN segment. Because of low throughputs hubs are now rarely used. Hub works on Layer-1 (Physical Layer) of OSI Model.

- **Switch** − A Switch is a multiport bridge and is used to connect hosts in a LAN segment. Switches are much faster than Hubs and operate on wire speed. Switch works on Layer-2 (Data Link Layer), but Layer-3 (Network Layer) switches are also available.
- **Router** − A router is Layer-3 (Network Layer) device which makes routing decisions for the data/information sent for some remote destination. Routers make the core of any interconnected network and the Internet.
- **Gateways** − A software or combination of software and hardware put together, works for exchanging data among networks which are using different protocols for sharing data.
- **Firewall** − Software or combination of software and hardware, used to protect users data from unintended recipients on the network/internet.

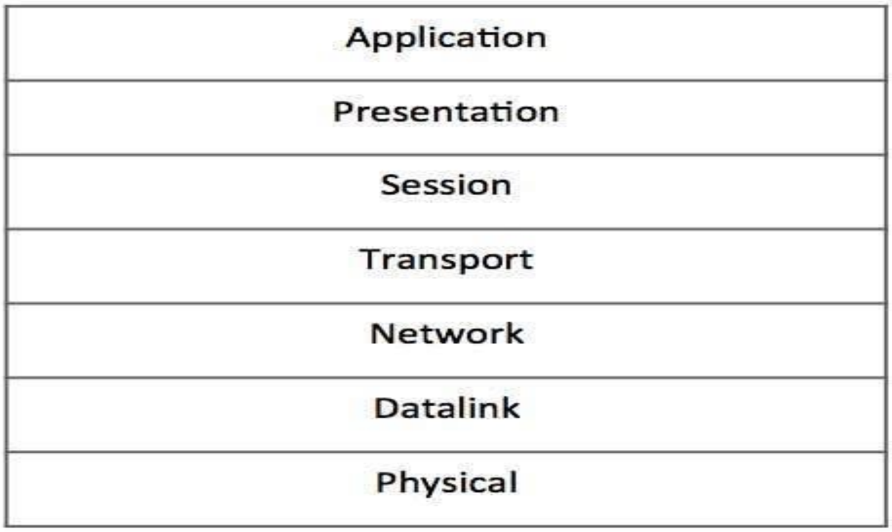
Host Addressing

Communication between hosts can happen only if they can identify each other on the network. In a single collision domain (where every packet sent on the segment by one host is heard by every other host) hosts can communicate directly via MAC address.

MAC address is a factory coded 48-bits hardware address which can also uniquely identify a host. But if a host wants to communicate with a remote host, i.e. not in the same segment or logically not connected, then some means of addressing is required to identify the remote host uniquely. A logical address is given to all hosts connected to Internet and this logical address is called **Internet Protocol Address**.

The International Standard Organization has a well-defined model for Communication Systems known as Open System Interconnection, or the OSI Model. This layered model is a conceptualized view of how one system should communicate with the other, using various protocols defined in each layer. Further, each layer is designated to a well-defined part of communication system. For example, the Physical layer defines all the components of physical nature, i.e. wires, frequencies, pulse codes, voltage transmission etc. of a communication system.

The OSI Model has the following seven layers −



Application
Presentation
Session
Transport
Network
Datalink
Physical

- **Application Layer (Layer-7)** − This is where the user application sits that needs to transfer data between or among hosts. For example − HTTP, file transfer application (FTP) and electronic mail etc.

- **Presentation Layer (Layer-6)** − This layer helps to understand data representation in one form on a host to other host in their native representation. Data from the sender is converted to on-the-wire data (general standard format) and at the receiver's end it is converted to the native representation of the receiver.
- **Session Layer (Layer-5)** − This layer provides session management capabilities between hosts. For example, if some host needs password verification for access and if credentials are provided then for that session password verification does not happen again. This layer can assist in synchronization, dialog control and critical operation management (e.g., an online bank transaction).
- **Transport Layer (Layer-4)** − This layer provides end to end data delivery among hosts. This layer takes data from the above layer and breaks it into smaller units called Segments and then gives it to the Network layer for transmission.
- **Network Layer (Layer-3)** − This layer helps to uniquely identify hosts beyond the subnets and defines the path which the packets will follow or be routed to reach the destination.
- **Data Link Layer (Layer-2)** − This layer takes the raw transmission data (signal, pulses etc.) from the Physical Layer and makes Data Frames, and sends that to the upper layer and vice versa. This layer also checks any transmission errors and sorts it out accordingly.
- **Physical Layer (Layer-1)** − This layer deals with hardware technology and actual communication mechanism such as signaling, voltage, cable type and length, etc.

Network Layer

The network layer is responsible for carrying data from one host to another. It provides means to allocate logical addresses to hosts, and identify them uniquely using the same. Network layer takes data units from Transport Layer and cuts them in to smaller unit called Data Packet.

Network layer defines the data path, the packets should follow to reach the destination. A router works on this layer and provides mechanism to route data to its destination.

A majority of the internet uses a protocol suite called the Internet Protocol Suite also known as the TCP/IP protocol suite. This suite is a combination of protocols which encompasses a number of different protocols for different purpose and need. Because the two major protocols in this suites are TCP (Transmission Control Protocol) and IP (Internet Protocol), this is commonly termed as TCP/IP Protocol suite. This protocol suite has its own reference model which it follows over the internet. In contrast with the OSI model, this model of protocols contains less layers.

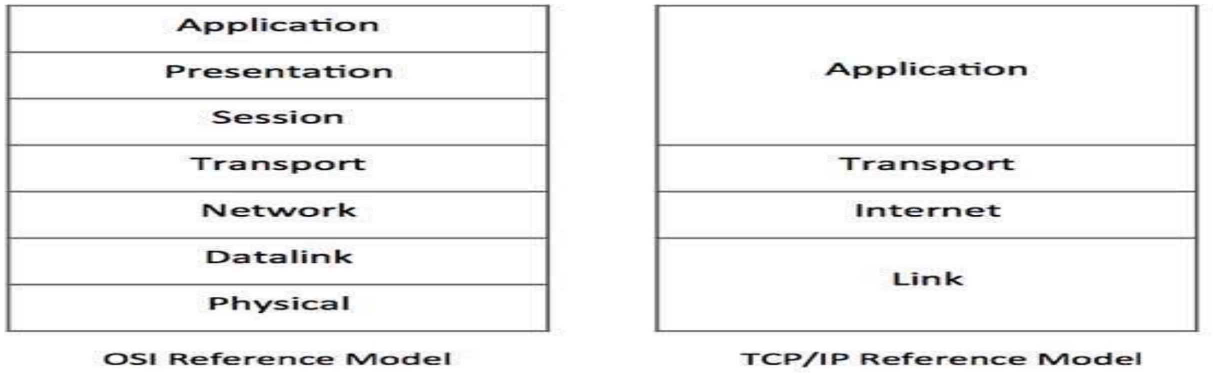


Figure − Comparative depiction of OSI and TCP/IP Reference Models

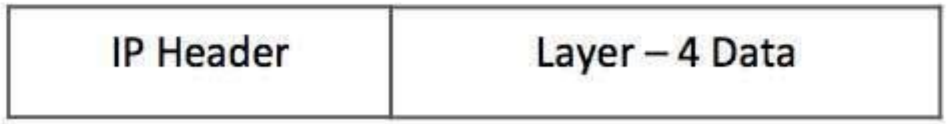
This model is indifferent to the actual hardware implementation, i.e. the physical layer of OSI Model. This is why this model can be implemented on almost all underlying technologies. Transport and Internet layers correspond to the same peer layers. All three top layers of OSI Model are compressed together in single Application layer of TCP/IP Model.

Internet Protocol Version 4 (IPv4)

Internet Protocol is one of the major protocols in the TCP/IP protocols suite. This protocol works at the network layer of the OSI model and at the Internet layer of the TCP/IP model. Thus this protocol has the responsibility of identifying hosts based upon their logical addresses and to route data among them over the underlying network.

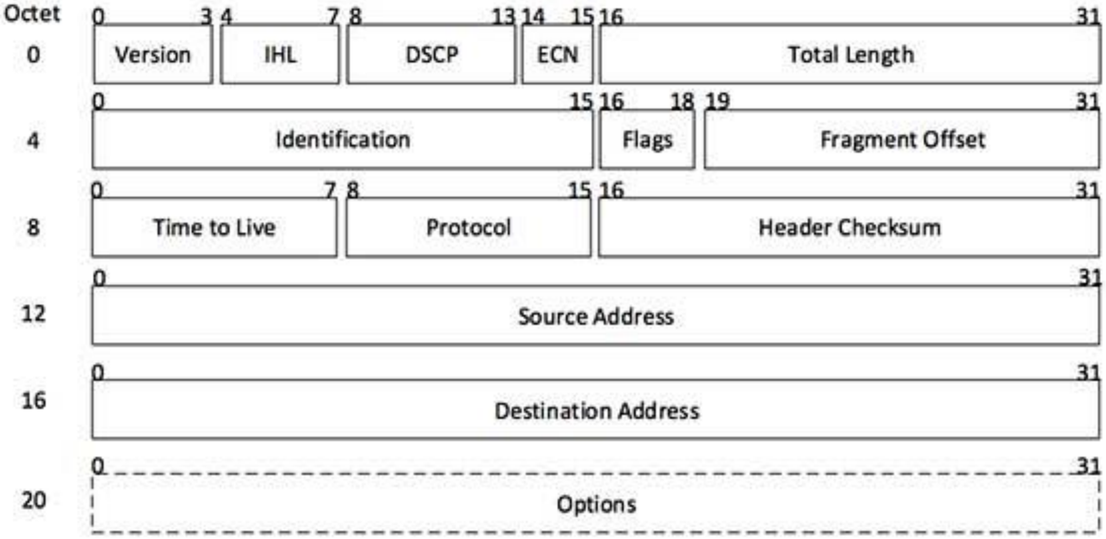
IP provides a mechanism to uniquely identify hosts by an IP addressing scheme. IP uses best effort delivery, i.e. it does not guarantee that packets would be delivered to the destined host, but it will do its best to reach the destination. Internet Protocol version 4 uses 32-bit logical address

Internet Protocol being a layer-3 protocol (OSI) takes data Segments from layer-4 (Transport) and divides it into packets. IP packet encapsulates data unit received from above layer and add to its own header information.



(IP Encapsulation)

The encapsulated data is referred to as IP Payload. IP header contains all the necessary information to deliver the packet at the other end.



[Image: IP Header]

IP header includes many relevant information including Version Number, which, in this context, is 4. Other details are as follows −

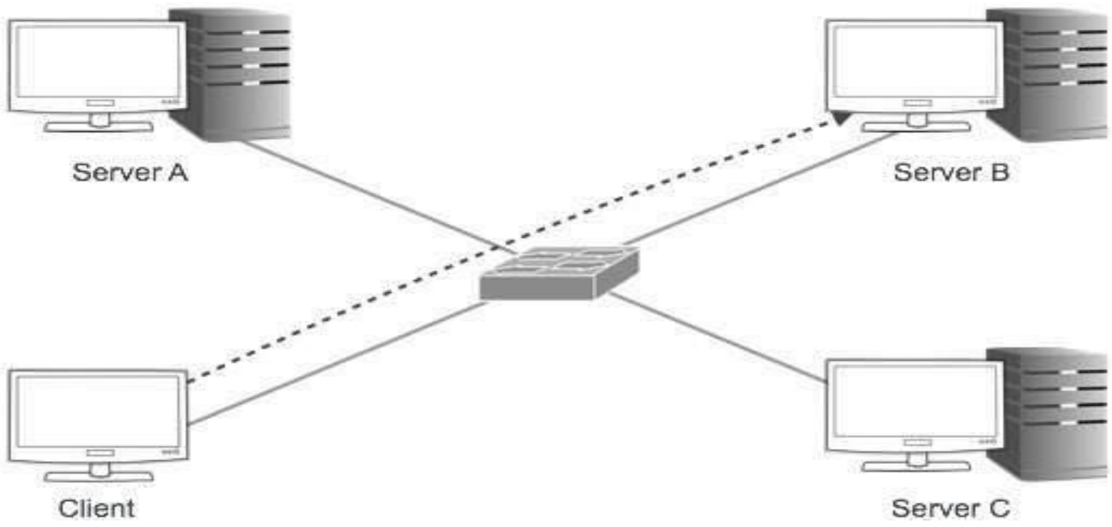
- **Version** − Version no. of Internet Protocol used (e.g. IPv4).

- **IHL** − Internet Header Length; Length of entire IP header.
- **DSCP** − Differentiated Services Code Point; this is Type of Service.
- **ECN** − Explicit Congestion Notification; It carries information about the congestion seen in the route.
- **Total Length** − Length of entire IP Packet (including IP header and IP Payload).
- **Identification** − If IP packet is fragmented during the transmission, all the fragments contain same identification number to identify original IP packet they belong to.
- **Flags** − As required by the network resources, if IP Packet is too large to handle, these 'flags' tells if they can be fragmented or not. In this 3-bit flag, the MSB is always set to '0'.
- **Fragment Offset** − This offset tells the exact position of the fragment in the original IP Packet.
- **Time to Live** − To avoid looping in the network, every packet is sent with some TTL value set, which tells the network how many routers (hops) this packet can cross. At each hop, its value is decremented by one and when the value reaches zero, the packet is discarded.
- **Protocol** − Tells the Network layer at the destination host, to which Protocol this packet belongs to, i.e. the next level Protocol. For example protocol number of ICMP is 1, TCP is 6 and UDP is 17.
- **Header Checksum** − This field is used to keep checksum value of entire header which is then used to check if the packet is received error-free.
- **Source Address** − 32-bit address of the Sender (or source) of the packet.
- **Destination Address** − 32-bit address of the Receiver (or destination) of the packet.
- **Options** − This is optional field, which is used if the value of IHL is greater than 5. These options may contain values for options such as Security, Record Route, Time Stamp, etc.

IPv4 supports three different types of addressing modes. −

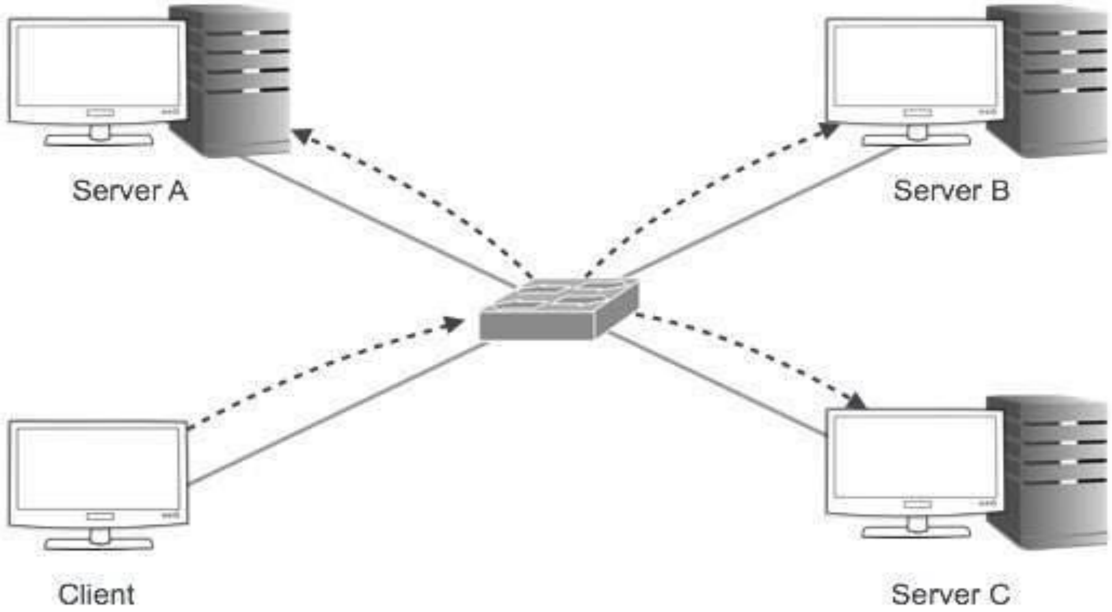
Unicast Addressing Mode

In this mode, data is sent only to one destined host. The Destination Address field contains 32- bit IP address of the destination host. Here the client sends data to the targeted server −



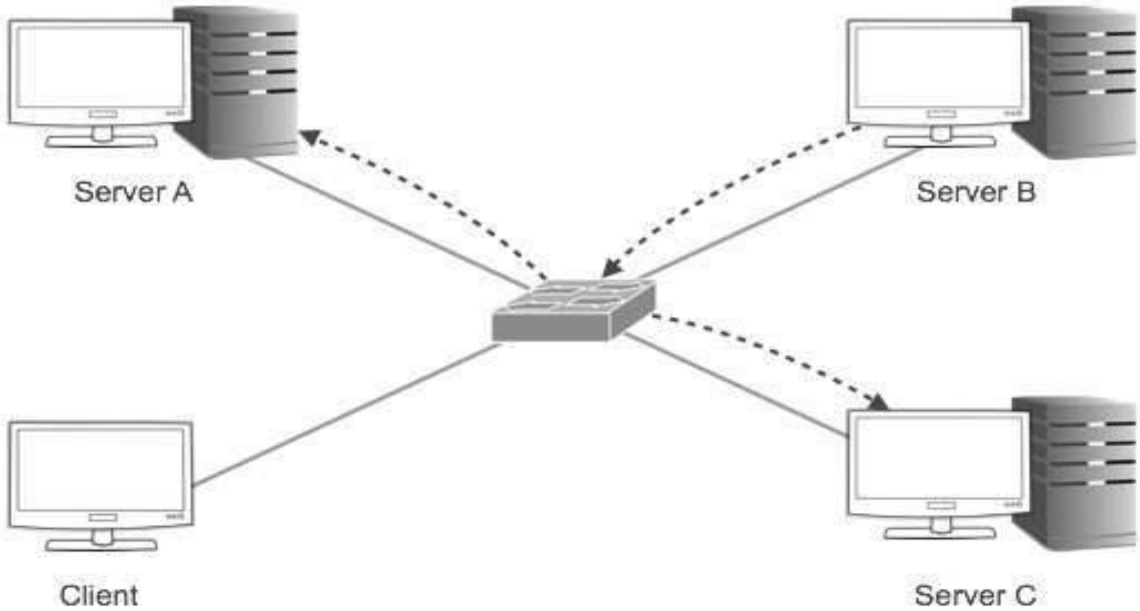
Broadcast Addressing Mode

In this mode, the packet is addressed to all the hosts in a network segment. The Destination Address field contains a special broadcast address, i.e. **255.255.255.255**. When a host sees this packet on the network, it is bound to process it. Here the client sends a packet, which is entertained by all the Servers −



Multicast Addressing Mode

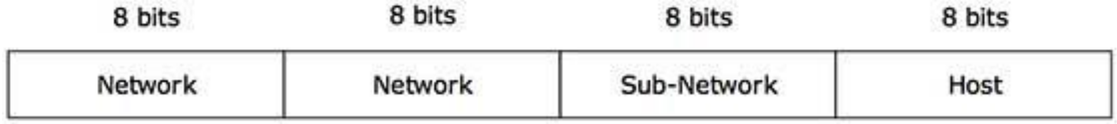
This mode is a mix of the previous two modes, i.e. the packet sent is neither destined to a single host nor all the hosts on the segment. In this packet, the Destination Address contains a special address which starts with 224.x.x.x and can be entertained by more than one host.



Here a server sends packets which are entertained by more than one servers. Every network has one IP address reserved for the Network Number which represents the network and one IP address reserved for the Broadcast Address, which represents all the hosts in that network.

Hierarchical Addressing Scheme

IPv4 uses hierarchical addressing scheme. An IP address, which is 32-bits in length, is divided into two or three parts as depicted −

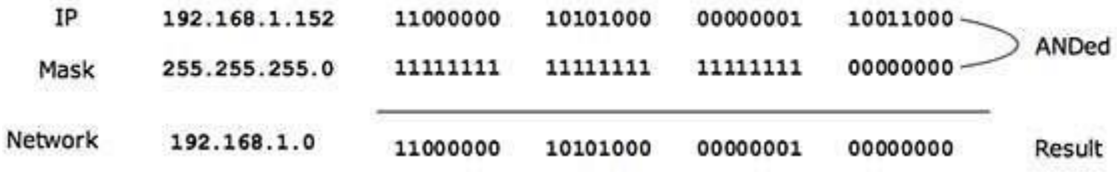


8 bits	8 bits	8 bits	8 bits
Network	Network	Sub-Network	Host

A single IP address can contain information about the network and its sub-network and ultimately the host. This scheme enables the IP Address to be hierarchical where a network can have many sub-networks which in turn can have many hosts.

Subnet Mask

The 32-bit IP address contains information about the host and its network. It is very necessary to distinguish both. For this, routers use Subnet Mask, which is as long as the size of the network address in the IP address. Subnet Mask is also 32 bits long. If the IP address in binary is ANDed with its Subnet Mask, the result yields the Network address. For example, say the IP Address is 192.168.1.152 and the Subnet Mask is 255.255.255.0 then −

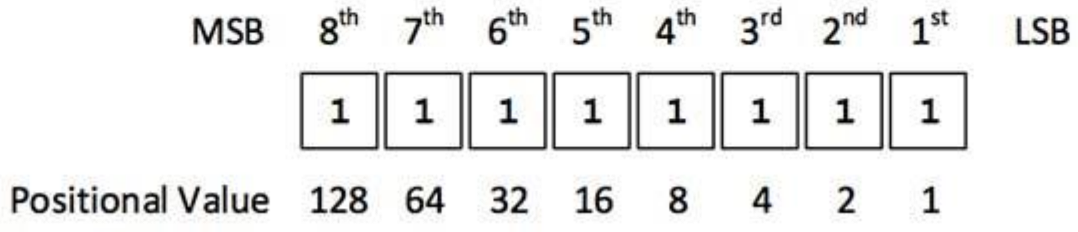


IP	192.168.1.152	11000000	10101000	00000001	10011000	ANDed
Mask	255.255.255.0	11111111	11111111	11111111	00000000	
Network	192.168.1.0	11000000	10101000	00000001	00000000	Result

This way the Subnet Mask helps extract the Network ID and the Host from an IP Address. It can be identified now that 192.168.1.0 is the Network number and 192.168.1.152 is the host on that network.

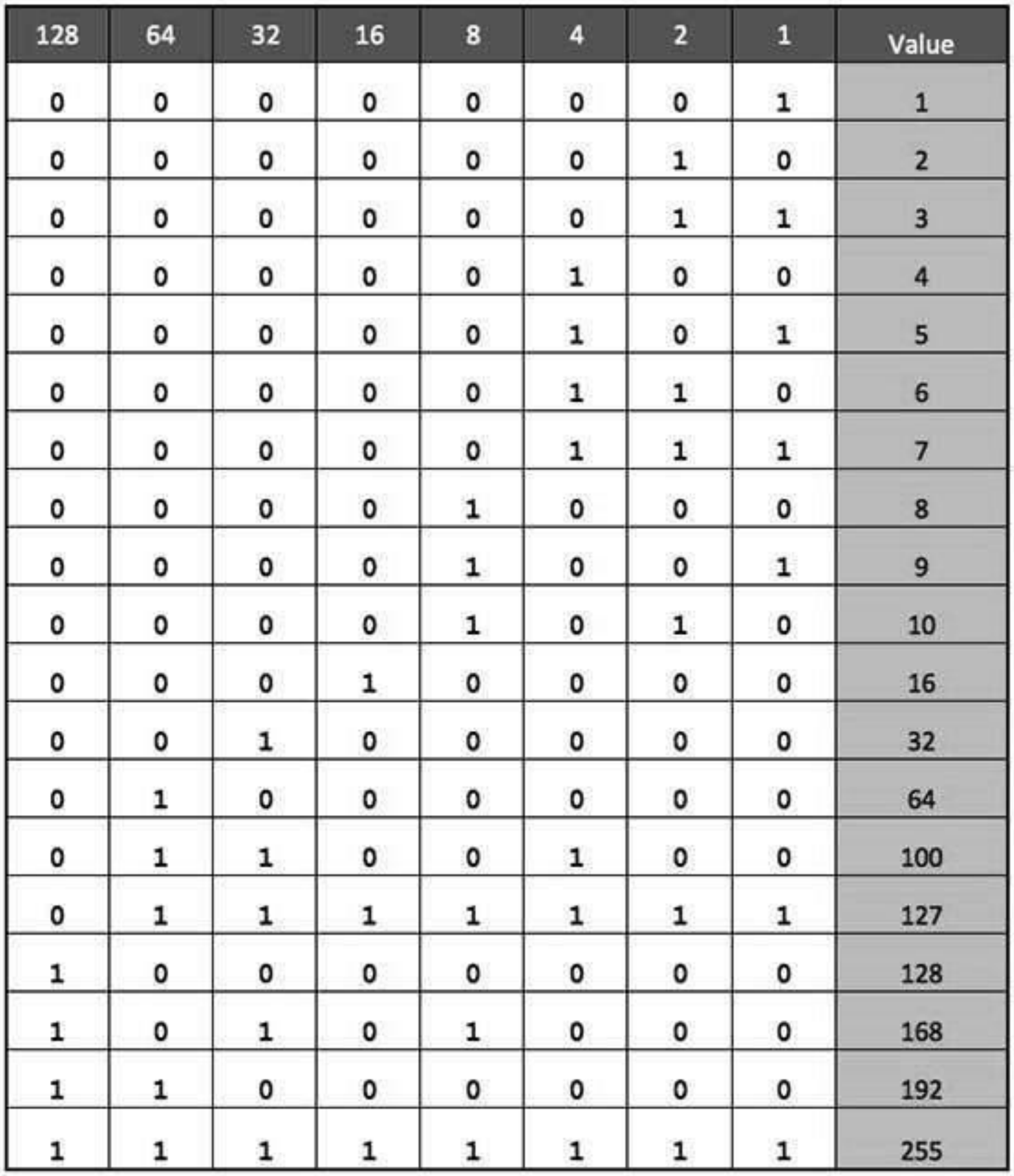
Binary Representation

The positional value method is the simplest form of converting binary from decimal value. IP address is 32 bit value which is divided into 4 octets. A binary octet contains 8 bits and the value of each bit can be determined by the position of bit value '1' in the octet.



MSB	8th	7th	6th	5th	4th	3rd	2nd	1st	LSB
	1	1	1	1	1	1	1	1	
Positional Value	128	64	32	16	8	4	2	1	

Positional value of bits is determined by 2 raised to power (position – 1), that is the value of a bit 1 at position 6 is 2^(6-1) that is 2^5 that is 32. The total value of the octet is determined by adding up the positional value of bits. The value of 11000000 is 128+64 = 192. Some examples are shown in the table below −

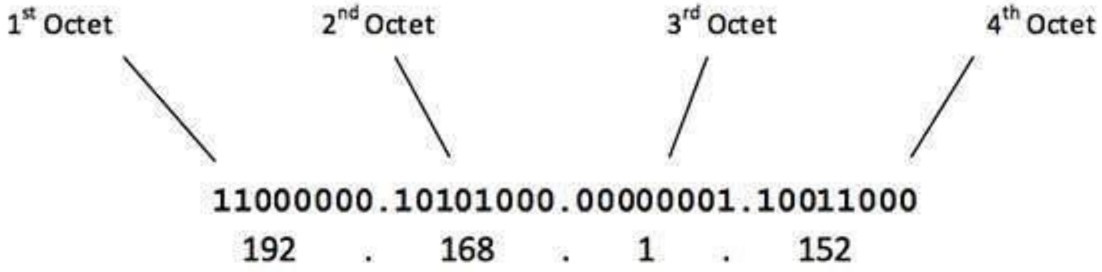


128	64	32	16	8	4	2	1	Value
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
0	0	0	0	0	1	1	1	7
0	0	0	0	1	0	0	0	8
0	0	0	0	1	0	0	1	9
0	0	0	0	1	0	1	0	10
0	0	0	1	0	0	0	0	16
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	1	0	0	100
0	1	1	1	1	1	1	1	127
1	0	0	0	0	0	0	0	128
1	0	1	0	1	0	0	0	168
1	1	0	0	0	0	0	0	192
1	1	1	1	1	1	1	1	255

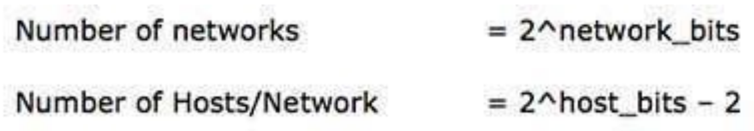
Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address.

Internet Corporation for Assigned Names and Numbers is responsible for assigning IP addresses.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −



The number of networks and the number of hosts per class can be derived by this formula −

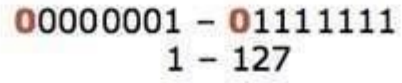


Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits – 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.



00000001 – 01111111
1 – 127

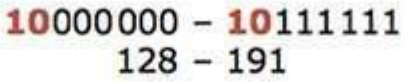
Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.



10000000 – 10111111
128 – 191

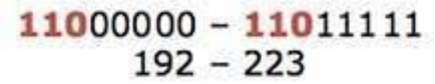
Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is −



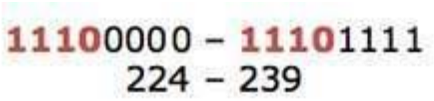
Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Class D Address

Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of −



Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

Class E Address

This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.

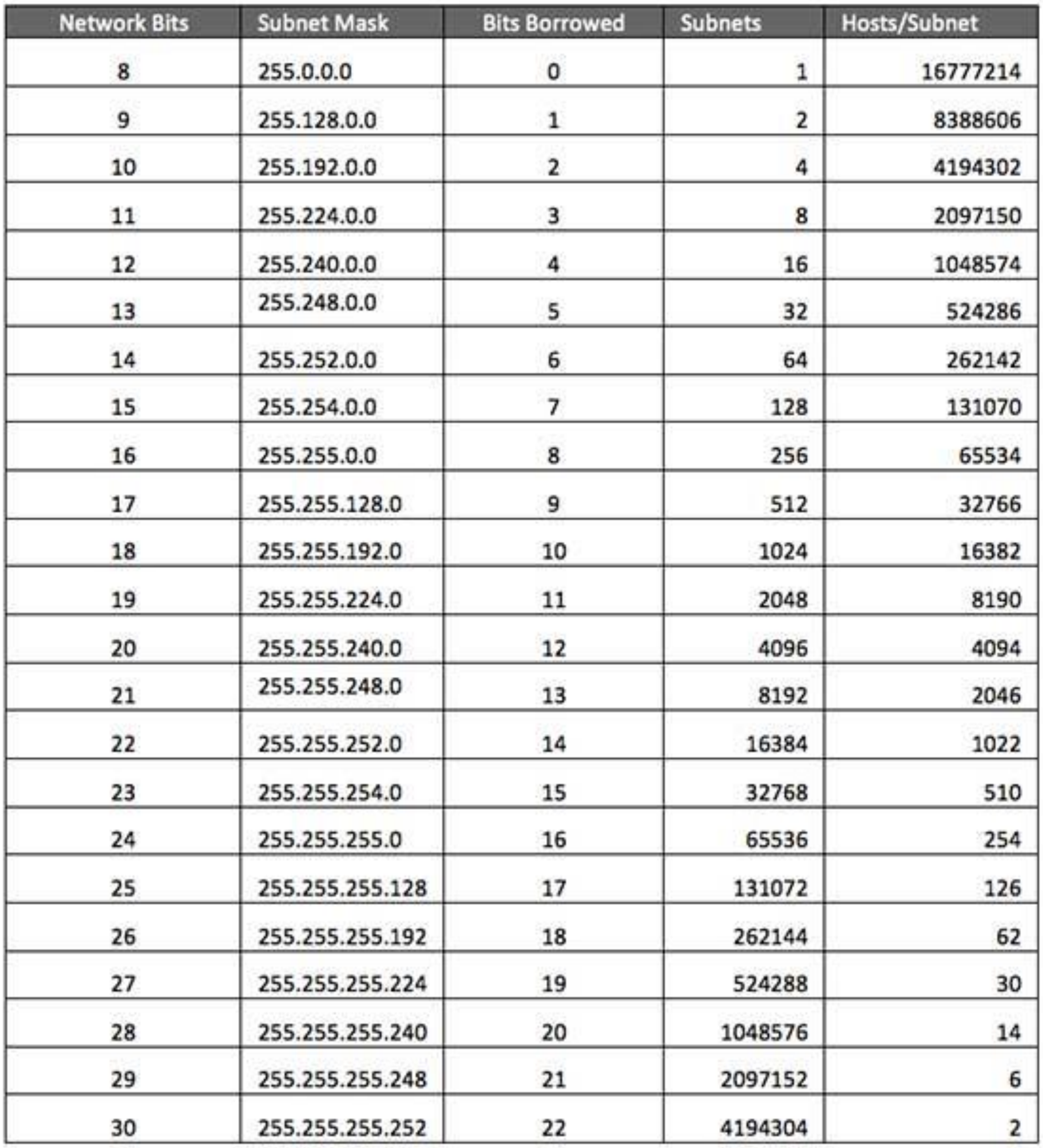
CIDR or **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Class A Subnets

In Class A, only the first octet is used as Network identifier and rest of three octets are used to be assigned to Hosts (i.e. 16777214 Hosts per Network). To make more subnet in Class A, bits from Host part are borrowed and the subnet mask is changed accordingly.

For example, if one MSB (Most Significant Bit) is borrowed from host bits of second octet and added to Network address, it creates two Subnets (2^{1}=2) with (2^{23}-2) 8388606 Hosts per Subnet.

The Subnet mask is changed accordingly to reflect subnetting. Given below is a list of all possible combination of Class A subnets −

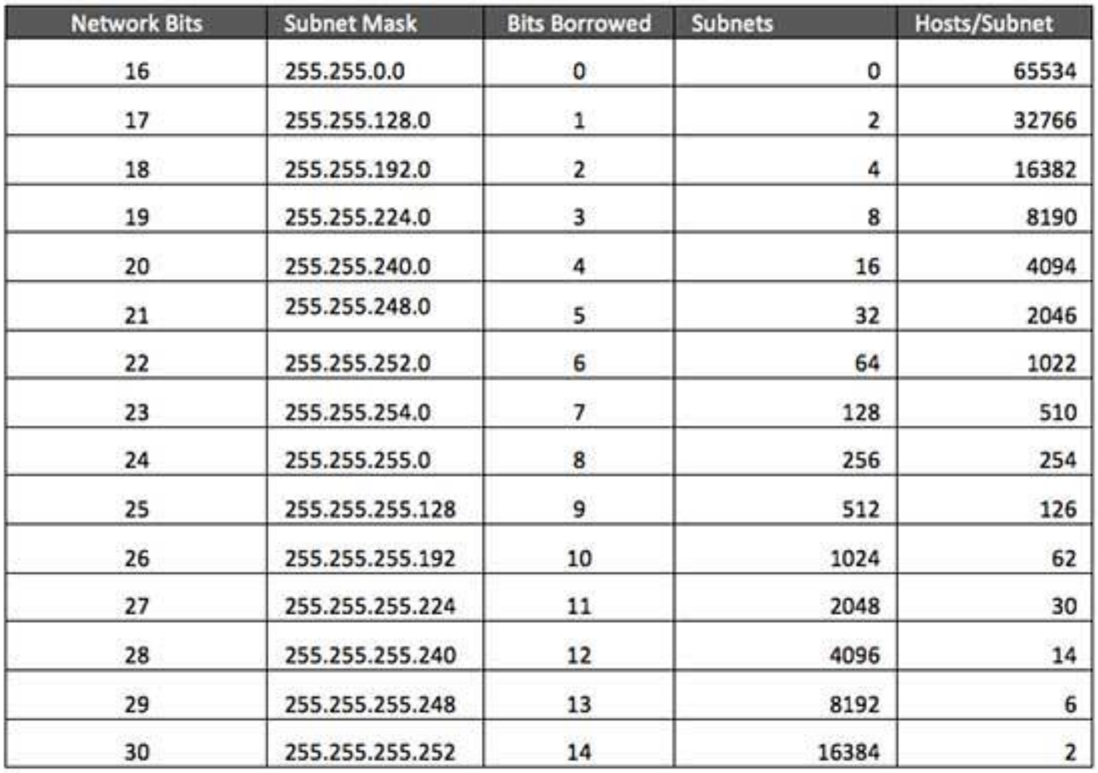


Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.255.240	20	1048576	14
29	255.255.255.248	21	2097152	6
30	255.255.255.252	22	4194304	2

In case of subnetting too, the very first and last IP address of every subnet is used for Subnet Number and Subnet Broadcast IP address respectively. Because these two IP addresses cannot be assigned to hosts, sub-netting cannot be implemented by using more than 30 bits as Network Bits, which provides less than two hosts per subnet.

Class B Subnets

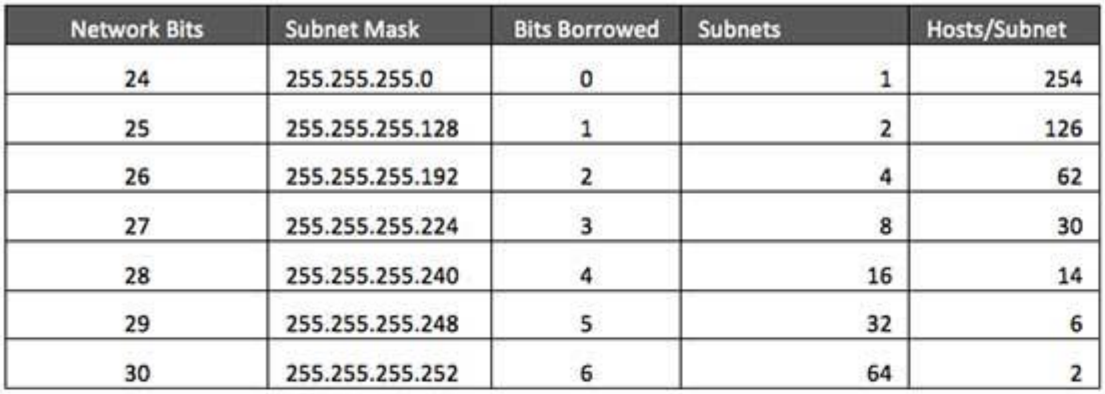
By default, using Classful Networking, 14 bits are used as Network bits providing (2^{14}) 16384 Networks and (2^{16}-2) 65534 Hosts. Class B IP Addresses can be subnetted the same way as Class A addresses, by borrowing bits from Host bits. Below is given all possible combination of Class B subnetting −



Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.255.240	12	4096	14
29	255.255.255.248	13	8192	6
30	255.255.255.252	14	16384	2

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address −



Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

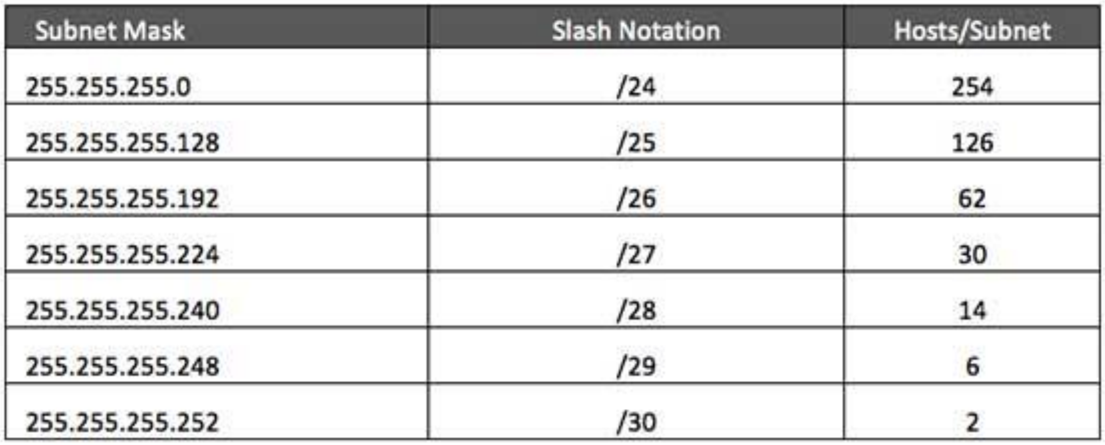
Internet Service Providers may face a situation where they need to allocate IP subnets of different sizes as per the requirement of customer. One customer may ask Class C subnet of 3 IP addresses and another may ask for 10 IPs. For an ISP, it is not feasible to divide the IP addresses into fixed size subnets, rather he may want to subnet the subnets in such a way which results in minimum wastage of IP addresses.

For example, an administrator have 192.168.1.0/24 network. The suffix /24 (pronounced as "slash 24") tells the number of bits used for network address. In this example, the administrator has three different departments with different number of hosts. Sales department has 100 computers, Purchase department has 50 computers, Accounts has 25 computers and Management has 5 computers. In CIDR, the subnets are of fixed size. Using the same methodology the administrator cannot fulfill all the requirements of the network.

The following procedure shows how VLSM can be used in order to allocate department-wise IP addresses as mentioned in the example.

Step - 1

Make a list of Subnets possible.



Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.255.240	/28	14
255.255.255.248	/29	6
255.255.255.252	/30	2

Step - 2

Sort the requirements of IPs in descending order (Highest to Lowest).

- Sales 100
- Purchase 50
- Accounts 25
- Management 5

Step - 3

Allocate the highest range of IPs to the highest requirement, so let's assign 192.168.1.0 /25 (255.255.255.128) to the Sales department. This IP subnet with Network number 192.168.1.0 has 126 valid Host IP addresses which satisfy the requirement of the Sales department. The subnet mask used for this subnet has 10000000 as the last octet.

Step - 4

Allocate the next highest range, so let's assign 192.168.1.128 /26 (255.255.255.192) to the Purchase department. This IP subnet with Network number 192.168.1.128 has 62 valid Host IP Addresses which can be easily assigned to all the PCs of the Purchase department. The subnet mask used has 11000000 in the last octet.

Step - 5

Allocate the next highest range, i.e. Accounts. The requirement of 25 IPs can be fulfilled with 192.168.1.192 /27 (255.255.255.224) IP subnet, which contains 30 valid host IPs. The network number of Accounts department will be 192.168.1.192. The last octet of subnet mask is 11100000.

Step - 6

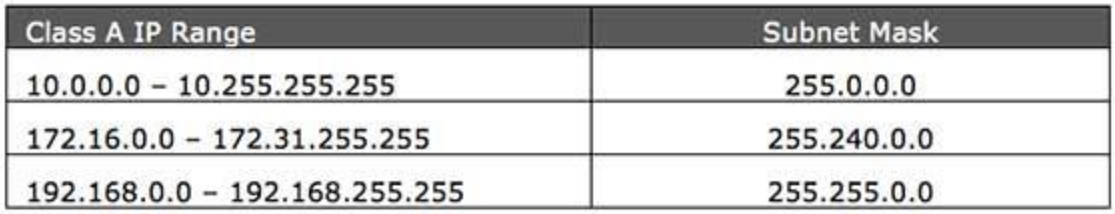
Allocate the next highest range to Management. The Management department contains only 5 computers. The subnet 192.168.1.224 /29 with the Mask 255.255.255.248 has exactly 6 valid host IP addresses. So this can be assigned to Management. The last octet of the subnet mask will contain 11111000.

By using VLSM, the administrators can subnet the IP subnet in such a way that least number of IP addresses are wasted. Even after assigning IPs to every department, the administrator, in this example, is still left with plenty of IP addresses which were not possible if he has used CIDR.

There are a few reserved IPv4 address spaces which cannot be used on the internet. These addresses serve special purpose and cannot be routed outside the Local Area Network.

Private IP Addresses

Every class of IP, (A, B & C) has some addresses reserved as Private IP addresses. These IPs can be used within a network, campus, company and are private to it. These addresses cannot be routed on the Internet, so packets containing these private addresses are dropped by the Routers.



Class A IP Range	Subnet Mask
10.0.0.0 – 10.255.255.255	255.0.0.0
172.16.0.0 – 172.31.255.255	255.240.0.0
192.168.0.0 – 192.168.255.255	255.255.0.0

In order to communicate with the outside world, these IP addresses must have to be translated to some public IP addresses using NAT process, or Web Proxy server can be used.

The sole purpose to create a separate range of private addresses is to control assignment of already-limited IPv4 address pool. By using a private address range within LAN, the requirement of IPv4 addresses has globally decreased significantly. It has also helped delaying the IPv4 address exhaustion.

IP class, while using private address range, can be chosen as per the size and requirement of the organization. Larger organizations may choose class A private IP address range where smaller organizations may opt for class C. These IP addresses can be further sub-netted and assigned to departments within an organization.

Loopback IP Addresses

The IP address range 127.0.0.0 – 127.255.255.255 is reserved for loopback, i.e. a Host's self-address, also known as localhost address. This loopback IP address is managed entirely by and within the operating system. Loopback addresses, enable the Server and Client processes on a single system to communicate with each other. When a process creates a packet with destination address as loopback address, the operating system loops it back to itself without having any interference of NIC.

Data sent on loopback is forwarded by the operating system to a virtual network interface within operating system. This address is mostly used for testing purposes like client-server architecture on a single machine. Other than that, if a host machine can successfully ping 127.0.0.1 or any IP from loopback range, implies that the TCP/IP software stack on the machine is successfully loaded and working.

Link-local Addresses

In case a host is not able to acquire an IP address from the DHCP server and it has not been assigned any IP address manually, the host can assign itself an IP address from a range of reserved Link-local addresses. Link local address ranges from 169.254.0.0 -- 169.254.255.255.

Assume a network segment where all systems are configured to acquire IP addresses from a DHCP server connected to the same network segment. If the DHCP server is not available, no host on the segment will be able to communicate to any other. Windows (98 or later), and Mac OS (8.0 or later) supports this functionality of self-configuration of Link-local IP address. In absence of DHCP server, every host machine randomly chooses an IP address from the above mentioned range and then checks to ascertain by means of ARP, if some other host also has not configured itself with the same IP address. Once all hosts are using link local addresses of same range, they can communicate with each other.

These IP addresses cannot help system to communicate when they do not belong to the same physical or logical segment. These IPs are also not routable.

Packet Flow in Network

All the hosts in IPv4 environment are assigned unique logical IP addresses. When a host wants to send some data to another host on the network, it needs the physical (MAC) address of the destination host. To get the MAC address, the host an broadcasts ARP message and asks to give the MAC address whoever is the owner of destination IP address. All the hosts on that segment receive the ARP packet, but only the host having its IP matching with the one in the ARP message, replies with its MAC address. Once the sender receives the MAC address of the receiving station, data is sent on the physical media.

In case the IP does not belong to the local subnet, the data is sent to the destination by means of Gateway of the subnet. To understand the packet flow, we must first understand the following components −

- **MAC Address** − Media Access Control Address is 48-bit factory hard coded physical address of network device which can uniquely be identified. This address is assigned by device manufacturers.

- **Address Resolution Protocol** − Address Resolution Protocol is used to acquire the MAC address of a host whose IP address is known. ARP is a Broadcast packet which is received by all the host in the network segment. But only the host whose IP is mentioned in ARP responds to it providing its MAC address.

- **Proxy Server** − To access the Internet, networks use a Proxy Server which has a public IP assigned. All the PCs request the Proxy Server for a Server on the Internet. The Proxy Server on behalf of the PCS sends the request to the server and when it receives a response from the Server, the Proxy Server forwards it to the client PC. This is a way to control Internet access in computer networks and it helps to implement web based policies.

- **Dynamic Host Control Protocol** − DHCP is a service by which a host is assigned IP address from a pre-defined address pool. DHCP server also provides necessary information such as Gateway IP, DNS Server Address, lease assigned with the IP, etc. By using DHCP services, a network administrator can manage assignment of IP addresses at ease.

- **Domain Name System** − It is very likely that a user does not know the IP address of a remote Server he wants to connect to. But he knows the name assigned to it, for example, tutorialpoints.com. When the user types the name of a remote server he wants to connect to, the localhost behind the screens sends a DNS query. Domain Name System is a method to acquire the IP address of the host whose Domain Name is known.
- **Network Address Translation** − Almost all PCs in a computer network are assigned private IP addresses which are not routable on the Internet. As soon as a router receives an IP packet with a private IP address, it drops it. In order to access servers on public private address, computer networks use an address translation service, which translates between public and private addresses, called Network Address Translation. When a PC sends an IP packet out of a private network, NAT changes the private IP address with public IP address and vice versa.

We can now describe the packet flow. Assume that a user wants to access www.TutorialsPoint.com from her personal computer. She has internet connection from her ISP. The following steps will be taken by the system to help her reach the destination website.

Step 1 – Acquiring an IP Address (DHCP)

When the user's PC boots up, it searches for a DHCP server to acquire an IP address. For the same, the PC sends a DHCPDISCOVER broadcast which is received by one or more DHCP servers on the subnet and they all respond with DHCPOFFER which includes all the necessary details such as IP, subnet, Gateway, DNS, etc. The PC sends DHCPREQUEST packet in order to request the offered IP address. Finally, the DHCP sends DHCPACK packet to tell the PC that it can keep the IP for some given amount of time that is known as IP lease.

Alternatively, a PC can be assigned an IP address manually without taking any help from DHCP server. When a PC is well configured with IP address details, it can communicate other computers all over the IP enabled network.

Step 2 – DNS Query

When a user opens a web browser and types www.tutorialpoints.com which is a domain name and a PC does not understand how to communicate with the server using domain names, then the PC sends a DNS query out on the network in order to obtain the IP address pertaining to the domain name. The pre-configured DNS server responds to the query with IP address of the domain name specified.

Step 3 – ARP Request

The PC finds that the destination IP address does not belong to his own IP address range and it has to forward the request to the Gateway. The Gateway in this scenario can be a router or a Proxy Server. Though the Gateway's IP address is known to the client machine but computers do not exchange data on IP addresses, rather they need the machine's hardware address which is Layer-2 factory coded MAC address. To obtain the MAC address of the Gateway, the client PC broadcasts an ARP request saying "Who owns this IP address?" The Gateway in response to the ARP query sends its MAC address. Upon receiving the MAC address, the PC sends the packets to the Gateway.

An IP packet has both source and destination addresses and it connects the host with a remote host logically, whereas MAC addresses help systems on a single network segment to transfer actual data. It is important that source and destination MAC addresses change as they travel across the Internet (segment by segment) but source and destination IP addresses never change.

The Internet Protocol version 4 was designed to be allocated to approximately 4.3 billion addresses. At the beginning of Internet this was considered a much wider address space for which there was nothing to worry about.

The sudden growth in internet users and its wide spread use has exponentially increased the number of devices which needs real and unique IP to be able to communicate. Gradually, an IPS is required by almost every digital equipment which were made to ease human life, such as Mobile Phones, Cars and other electronic devices. The number of devices (other than computers/routers) expanded the demand for extra IP addresses, which were not considered earlier.

Allocation of IPv4 is globally managed by Internet Assigned Numbers Authority (IANA) under coordination with the Internet Corporation for Assigned Names and Numbers (ICANN). IANA works closely with Regional Internet Registries, which in turns are responsible for efficiently distributing IP addresses in their territories. There are five such RIRS. According to IANA reports, all the IPv4 address blocks have been allocated. To cope up with the situation, the following practices were being done −

- **Private IPs −** Few blocks of IPs were declared for private use within a LAN so that the requirement for public IP addresses can be reduced.
- **NAT −** Network address translation is a mechanism by which multiple PCs/hosts with private IP addresses are enabled to access using one or few public IP addresses.
- Unused Public IPs was reclaimed by RIRs.

Internet Protocol v6 (IPv6)

IETF (Internet Engineering Task Force) has redesigned IP addresses to mitigate the drawbacks of IPv4. The new IP address is version 6 which is 128-bit address, by which every single inch of the earth can be given millions of IP addresses.

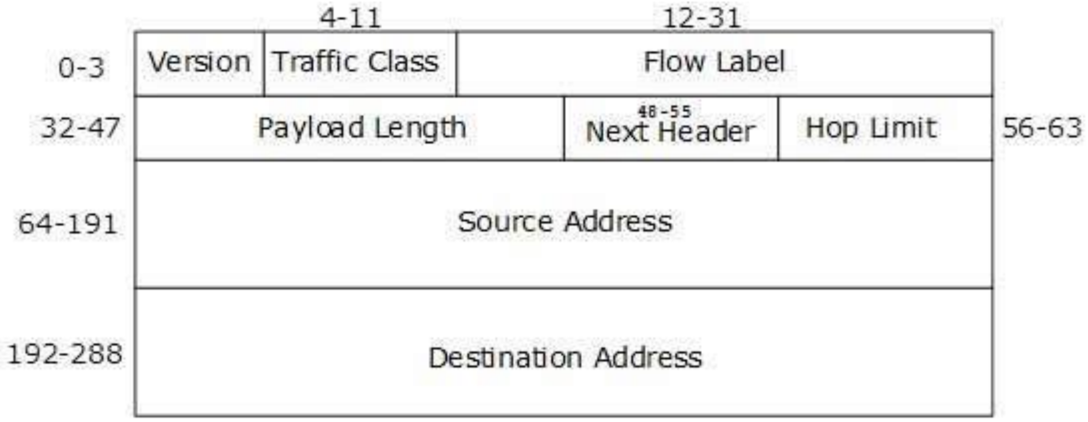
Today majority of devices running on Internet are using IPv4 and it is not possible to shift them to IPv6 in the coming days. There are mechanisms provided by IPv6, by which IPv4 and IPv6 can co-exist unless the Internet entirely shifts to IPv6 −

- Dual IP Stack
- Tunneling (6to4 and 4to6)
- NAT Protocol Translation

IPV6 Header

The wonder of IPv6 lies in its header. An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

Fixed Header



IPv6 fixed header is 40 bytes long and contains the following information.

Sr.No.	Field & Description
1	**Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
2	**Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3	**Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.
5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

Key Differences between IPv4 and IPv6

Let us look at the substantial difference between IPv4 and IPv6.

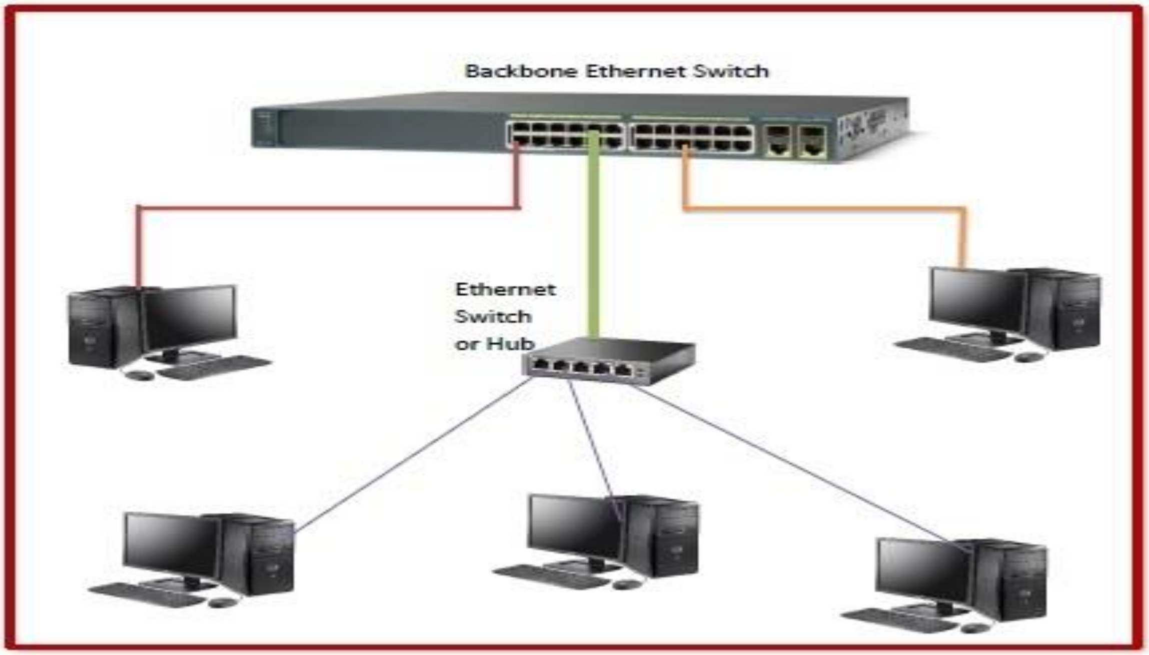
1. IPv4 has 32-bit address length whereas IPv6 has 128-bit address length.
2. IPv4 addresses represent the binary numbers in decimals. On the other hand, IPv6 addresses express binary numbers in hexadecimal.
3. IPv6 uses end-to-end fragmentation while IPv4 requires an intermediate router to fragment any datagram that is too large.
4. Header length of IPv4 is 20 bytes. In contrast, header length of IPv6 is 40 bytes.
5. IPv4 uses checksum field in the header format for handling error checking. On the contrary, IPv6 removes the header checksum field.
6. In IPv4, the base header does not contain a field for header length, and 16-bit payload length field replaces it in the IPv6 header.
7. The option fields in IPv4 are employed as extension headers in IPv6.
8. The Time to live field in IPv4 refers to as Hop limit in IPv6.
9. The header length field which is present in IPv4 is eliminated in IPv6 because the length of the header is fixed in this version.
10. IPv4 uses broadcasting to transmit the packets to the destination computers while IPv6 uses multicasting and any casting.
11. IPv6 provides authentication and encryption, but IPv4 doesn’t provide it.

UNIT – 4 (NETWORK ARCHITECTURE)

Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s as IEEE 802.3 standard. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

In switched Ethernet, the hub connecting the stations of the classic Ethernet is replaced by a switch. The switch connects the high-speed backplane bus to all the stations in the LAN. The switch-box contains a number of ports, typically within the range of 4 – 48. A station can be connected in the network by simply plugging a connector to any of the ports. Connections from a backbone Ethernet switch can go to computers, peripherals or other Ethernet switches and Ethernet hubs.

The following diagram shows configuration of a switched Ethernet −



Working Principle

Unlike classic Ethernet in which the channel is shared by the stations, in switched Ethernet, each station gets a dedicated connection. When a port of the switch receives a frame, it checks the destination address in the frame and then sends the frame to the corresponding port, for outgoing data.

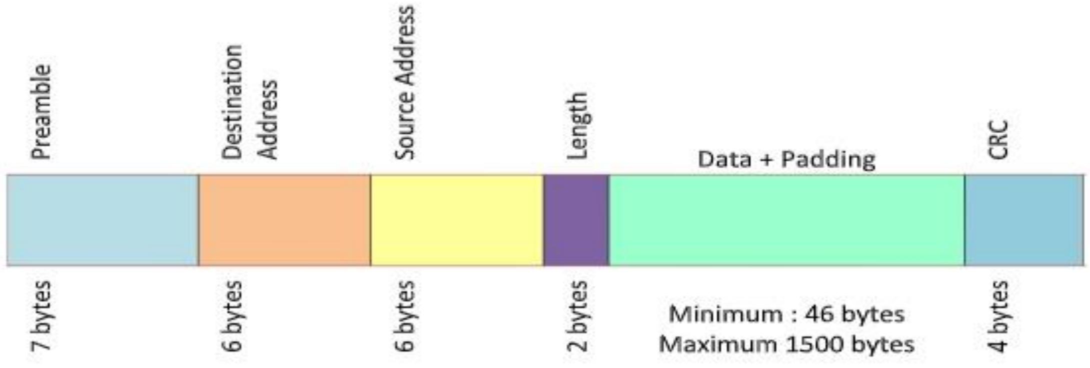
In switched Ethernet, collisions do not occur in the channel due to the presence of dedicated connection to each station. However, collisions may still occur in a destination port if it receives frames from more than one ports simultaneously. In a switch, each port has its own individual collision domain and resolves it individually.

Frame Format of Switched Ethernet

The frame format of switched Ethernet is same as that of classic Ethernet. The fields are −

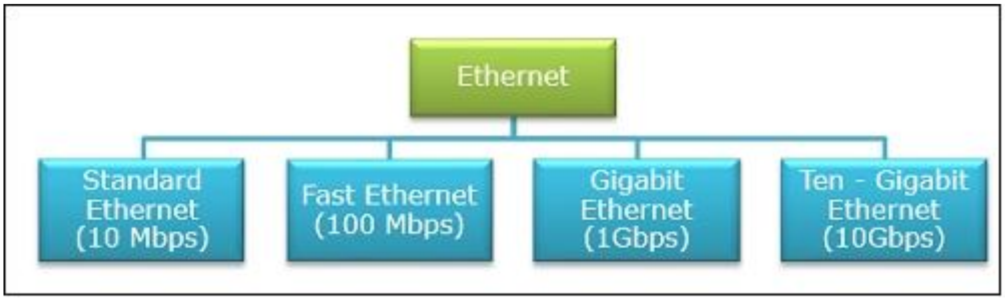
- **Preamble:** An 8 bytes starting field that provides alert and timing pulse for transmission.
- **Destination Address:** A 6 byte field containing physical address of destination stations.

- **Source Address**: A 6 byte field containing the physical address of the sending station.
- **Length**: A 2 bytes field that stores the number of bytes in the data field.
- **Data:** A variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding:** Extra bits added to the data to bring its length to the minimum size of 46 bytes.
- **CRC:** A 4 byte field that contains the error detection information.



Switched Ethernet Frame Format

Ethernet is a set of technologies and protocols that are used primarily in LANs. However, Ethernet can also be used in MANs and even WANs. It was first standardized in the 1980s as IEEE 802.3 standard. Since then, it has gone through four generations, as shown in the following chart

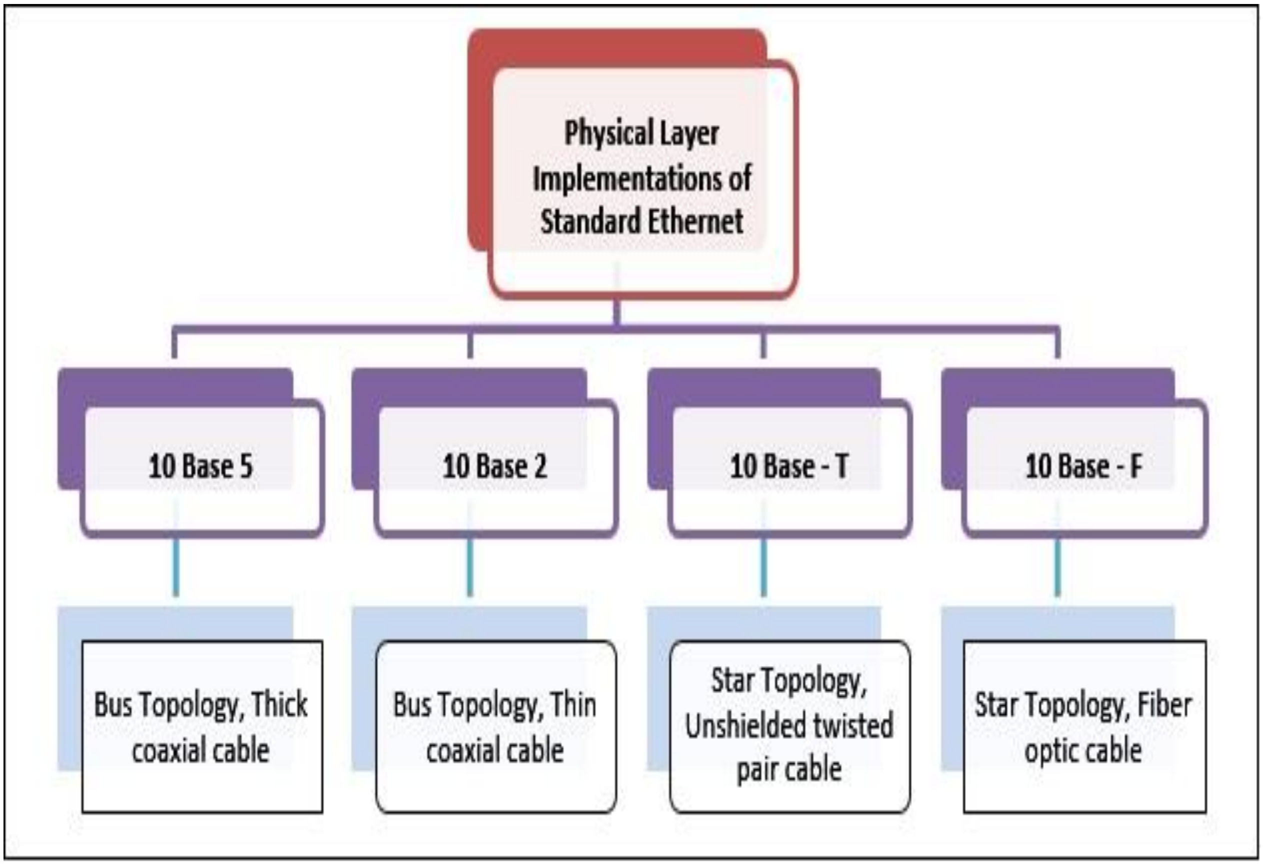


Standard Ethernet is also referred to as Basic Ethernet. It uses 10Base5 coaxial cables for communications. Ethernet provides service up to the data link layer. At the data link layer, Ethernet divides the data stream received from the upper layers and encapsulates it into frames, before passing them on to the physical layer.

The main parts of an Ethernet frame are

- **Preamble –** It is the starting field that provides alert and timing pulse for transmission.
- **Destination Address –** It is a 6-byte field containing the physical address of destination stations.
- **Source Address –** It is a 6-byte field containing the physical address of the sending station.
- **Length –** It stores the number of bytes in the data field.
- **Data and Padding –** This carries the data from the upper layers.
- **CRC –** It contains error detection information.

Standard Ethernet has many physical layer implementations. The four main physical layer implementations are shown in the following diagram


Physical Layer Implementations of Standard Ethernet
10 Base 5
10 Base 2
10 Base - T
10 Base - F
Bus Topology, Thick coaxial cable
Bus Topology, Thin coaxial cable
Star Topology, Unshielded twisted pair cable
Star Topology, Fiber optic cable

Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s as IEEE 802.3 standard. Ethernet is classified into two categories: classic Ethernet and switched Ethernet.

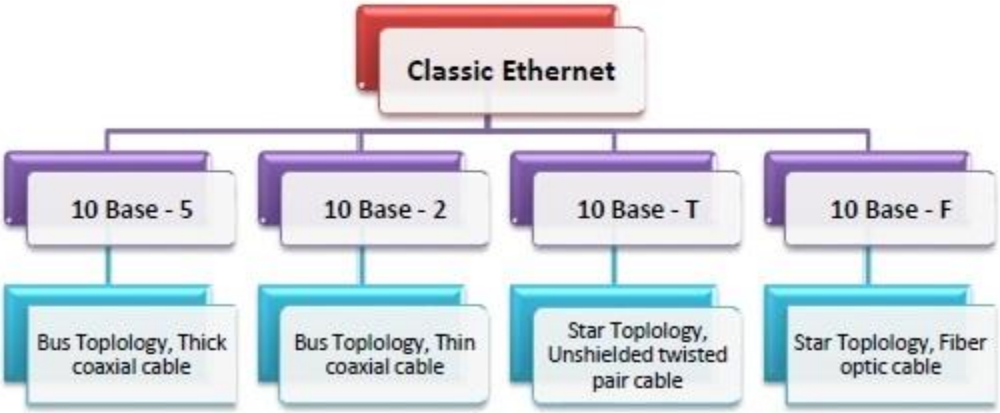
Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used. Most varieties of classic Ethernet have become obsolete in present communication scenario.

Varieties of Classic Ethernet

The common varieties of classic Ethernet are -

- **Thick coax (10BASE-5)**: This was the original version that used a single coaxial cable into which a connection can be tapped by drilling into the cable to the core. The 5 refers to the maximum segment length of 500m.
- **Thin coax (10BASE-2)**: This is a thinner variety where segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **Twisted pair (10BASE-T)**: This uses unshielded twisted pair copper wires as physical layer medium.

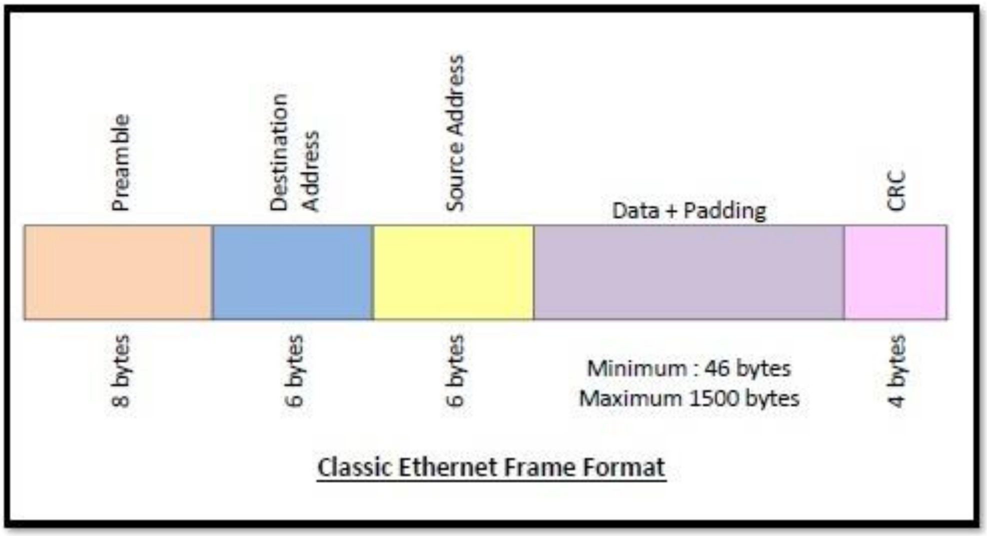
- **Ethernet over Fiber (10BASE-F):** This uses fiber optic cables as medium of transmission.


Classic Ethernet
10 Base - 5
10 Base - 2
10 Base - T
10 Base - F
Bus Toplology, Thick coaxial cable
Bus Toplology, Thin coaxial cable
Star Toplology, Unshielded twisted pair cable
Star Toplology, Fiber optic cable

Frame Format of Classic Ethernet

The main fields of a frame of classic Ethernet are -

- **Preamble**: It is a 8 bytes starting field that provides alert and timing pulse for transmission.
- **Destination Address**: It is a 6 byte field containing physical address of destination stations.
- **Source Address**: It is a 6 byte field containing the physical address of the sending station.
- **Length**: It a 7 bytes field that stores the number of bytes in the data field.
- **Data**: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- **Padding**: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- **CRC**: CRC stands for cyclic redundancy check. It contains the error detection information.



Thick Ethernet

Thick Ethernet was the first commercially available form of cabling supported by Ethernet. It is technically known as 10-BASE-5. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500 metres (1,600 ft). This type of cabling allows 100 stations to be connected to it by vampire taps.

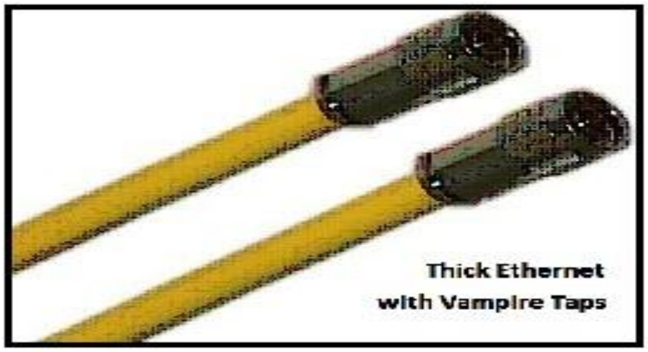
Thin Ethernet

Thin Ethernet, popularly known as cheapernet or thinnet, is among the family of Ethernet standards that uses thinner coaxial cable as a transmission media. It is technically known as 10-BASE-2.

Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 2 refers to the maximum segment length of about 200 metres (precisely 185 metres). This type of cabling allows a maximum of 30 stations to be connected to it by BNC connectors with 50 centimetres minimum gap between subsequent stations.

Differences between Thick Ethernet and Thin Ethernet

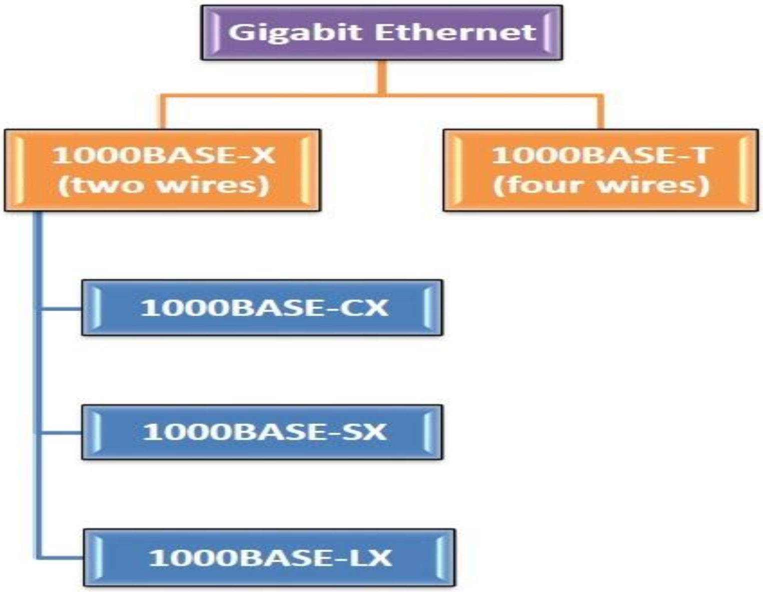
Thick Ethernet	Thin Internet
It is technically known as 10-BASE-5.	It is technically known as 10-BASE-5.
The maximum segment length is 500 metres.	The maximum segment length is nearly 200 metres (185 m to be exact).
It uses the thick coaxial cable RG-8/U.	It uses the thinner coaxial cable RG-58/AU.
Connectors used are vampire taps.	Connectors used are BNC connectors.
It allows a maximum of 100 stations to be connected.	It allows a maximum of 30 stations to be connected.



In computer networks, Gigabit Ethernet (GbE) is the family of Ethernet technologies that achieve theoretical data rates of 1 gigabit per second (1 Gbps). It was introduced in 1999 and was defined by the IEEE 802.3ab standard.

Varieties of Gigabit Ethernet

The popular varieties of fast Ethernet are 1000Base-SX, 1000Base-LX, 1000BASE-T and 1000Base-CX.



1000BASE-CX

- Defined by IEEE 802.3z standard
- The initial standard for Gigabit Ethernet
- Uses shielded twisted pair cables with DE-9 or 8P8C connector
- Maximum segment length is 25 metres
- Uses NRZ line encoding and 8B/6B block encoding

1000BASE-SX

- Defined by IEEE 802.3z standard
- Uses a pair of fibre optic cables of a shorter wavelength having 770 – 860 nm diameter
- The maximum segment length varies from 220 – 550 metres depending upon the fiber properties.
- Uses NRZ line encoding and 8B/10B block encoding

1000BASE-LX

- Defined by IEEE 802.3z standard
- Uses a pair of fibre optic cables of a longer wavelength having 1270 – 1355 nm diameter
- Maximum segment length is 500 metres
- Can cover distances up to 5 km
- Uses NRZ line encoding and 8B/10B block encoding

1000BASE-T

- Defined by IEEE 802.3ab standard
- Uses a pair four lanes of twisted-pair cables (Cat-5, Cat-5e, Cat-6, Cat-7)
- Maximum segment length is 100 metres
- Uses trellis code modulation technique

UNIT – 5 (NETWORK CONNECTIVITY)

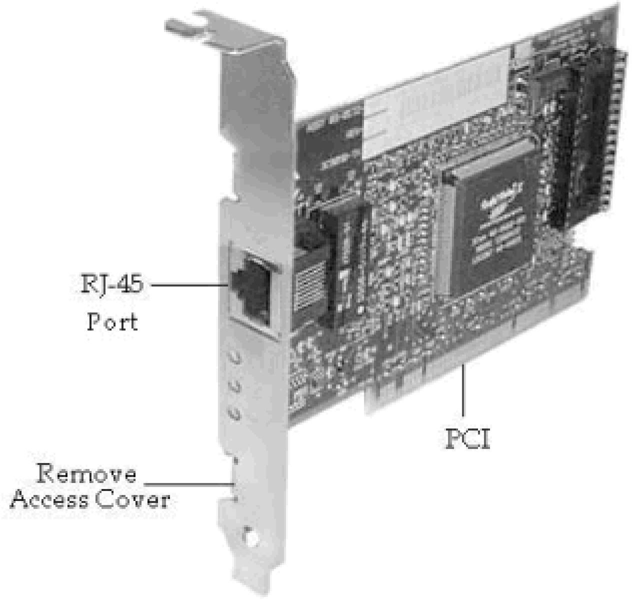
Connectivity is a term closely related to network because without connectivity a network is of no use. Connectivity refers to the degree to which any given computer or application can cooperate with other network components.

The Network connectivity devices are:

- The Network Interface card (NIC)
- The hub
- The switch
- The bridge
- Transceivers
- Wireless access points
- The router
- The gateway

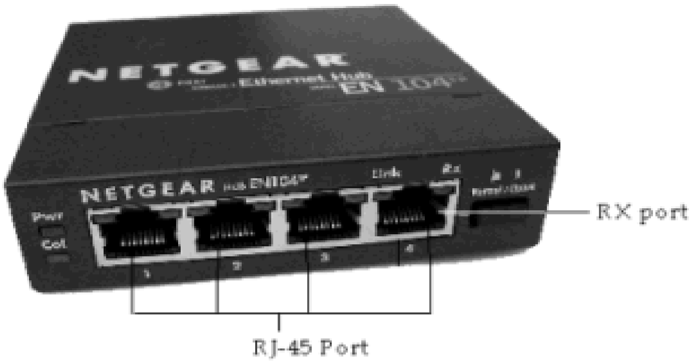
Network Interface Card (NIC): The Network Interface Card (NIC) used connects the computer to the external network. It will normally have a PCI connector (Edge connector) to connect to one of the PC expansion slots, and an RJ-45 connector to connect to external Ethernet. Note that the interface connectors may differ depending upon the expansion bus being used (for example, PCI, ISA, EISA, USB etc.), and the networking media being used (for example, 10Base2, 10Base5, 10BaseT, etc.). Each of these has their own interface specifications. Almost all NICs have LED indicators showing the network connectivity.

A commonly used Network Interface Card is shown in the figure below.



Network Interface Card Model

Hub: A Hub connects all the nodes of a network using Twisted Pair (UTP or STP) cables. In a Hub, the signals received on one port are transmitted to all other ports, and vice versa. All nodes (work stations) connected using a Hub can listen to one another all the time. The advantage of using a Hub is low cost, and easy integration. The disadvantage is reduced bandwidth, and data security. The reduction in bandwidth comes due to the fact that all workstations are in the same collision domain. If two or more workstations try to transmit during the same time, it results in collision of signals, and the signals are lost altogether. As a result, the available bandwidth of the Ethernet network is reduced.



A 4-port Hub is shown in the figure.

Switch: Switch is a network device that connects other devices to Ethernet networks through twisted pair cables. It uses packet switching technique to receive, store and forward data packets on the network. The switch maintains a list of network addresses of all the devices connected to it.

On receiving a packet, it checks the destination address and transmits the packet to the correct port. Before forwarding, the packets are checked for collision and other network errors. The data is transmitted in full duplex mode

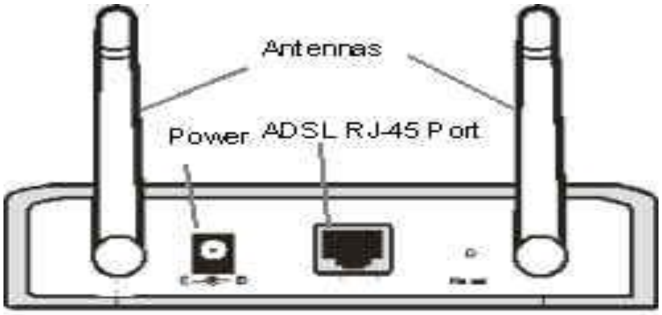
Data transmission speed in switches can be double that of other network devices like hubs used for networking. This is because switch shares its maximum speed with all the devices connected to it. This helps in maintaining network speed even during high traffic. In fact, higher data speeds are achieved on networks through use of multiple switches.

48-port Switch

Bridge: A Bridge functions very similar to a Switch. It segments a given network according to the requirements. Segmentation using a Bridge enables keeping un-intended traffic from entering different segments of a network. Both Bridge and Switch are OSI layer-2 devices. Bridges filter traffic based on the destination address of the frame. If a frame's destination is a node on the same segment where it originated, it is not forwarded. If it is destined for a node on another LAN, it is connected to corresponding bridge port and forwarded to that port.

Transceivers: Transceivers are commonly used with co-axial media using 10Base2 or 10Base5 networking standards. It allows a Network Interface Card to connect to a coax, providing necessary translation of signals.

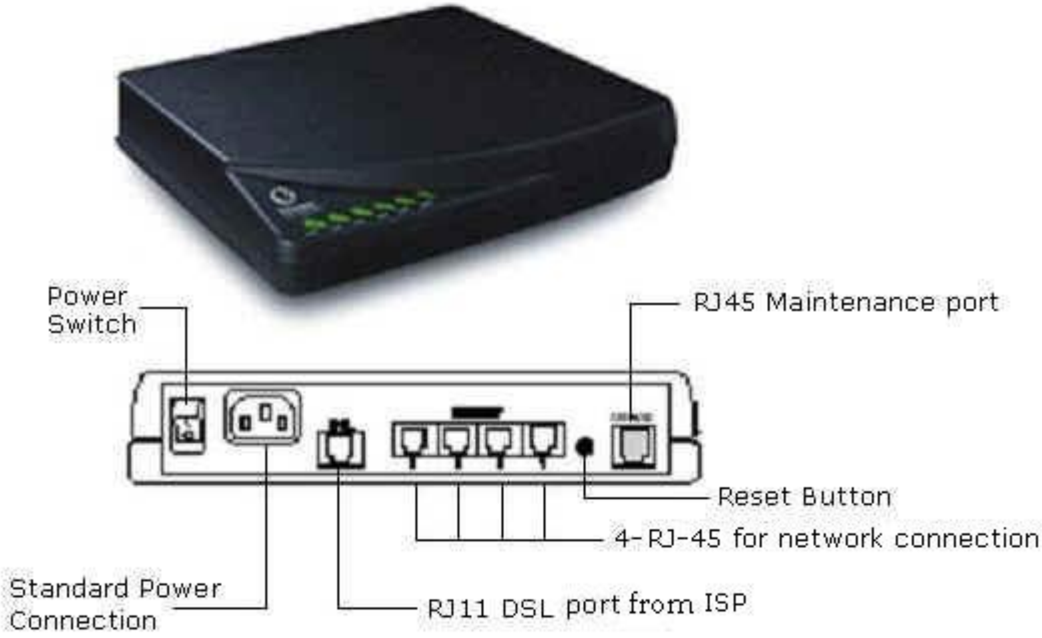
Wireless Access Points (WAP): A wireless access point allows mobile users to connect to a central network node without using any wires. Wireless connectivity is useful for mobile workstations, since there is no wiring involved. The wireless access standards are broadly divided into 802.11a, 802.11b, and 802.11g. 802.11g is most popular among these due to high bandwidth that it provides, and the availability of hardware. A commercially available wireless access point is shown in the figure below.



Back-panel

A WAP device

Router: A Router connects multiple networks, and uses routing to forward packets. It is a OSI Layer-3 device and works on the logical address of a host or a node. Compare this with a Switch which works on the physical address (such as MAC address) of a host or a node. A simple DSL router is shown in the figure below.



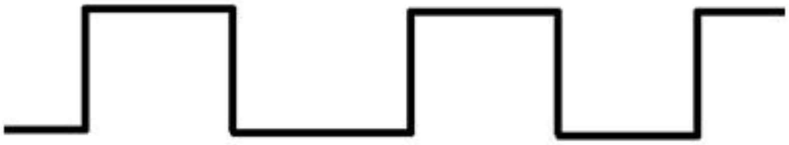
Router

Gateways: Gateway is a network device used to connect two or more dissimilar networks. In networking parlance, networks that use different protocols are dissimilar networks. A gateway usually is a computer with multiple NICs connected to different networks. A gateway can also be configured completely using software. As networks connect to a different network through gateways, these gateways are usually hosts or end points of the network.

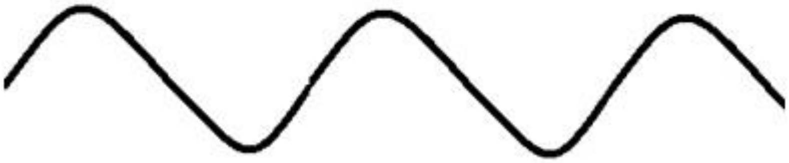
Gateway uses packet switching technique to transmit data from one network to another. In this way it is similar to a router, the only difference being router can transmit data only over networks that use same protocols.

Gateways are the most complex devices with respect to the functionality. They typically work at the upper most layers of OSI model. A gateway is used to connect two different environments, such as a Frame-Relay network and an X.25 network.

Modems: Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.



Digital Data Waveform



Analog Data Waveform

The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − **modulator** and **demodulator**. The **modulator** converts digital data into analog data when the data is being sent by the computer. The **demodulator** converts analog data signals into digital data when it is being received by the computer.

Types of Modem

Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.

Depending on direction of data transmission, modem can be of these types −

- **Simplex** − A simplex modem can transfer data in only one direction, from digital device to network (modulator) or network to digital device (demodulator).
- **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

Multiplexing in Computer Networks

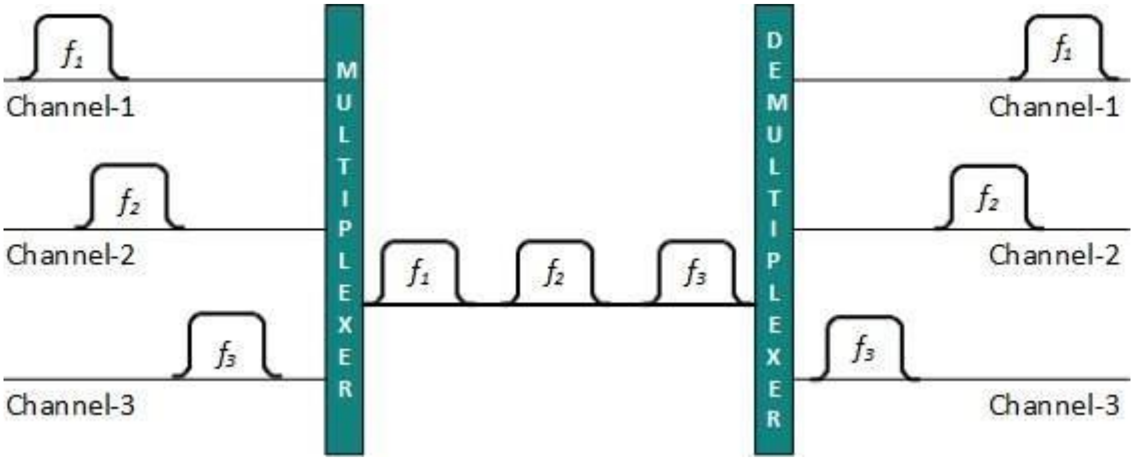
Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams.

Communication is possible over the air (radio frequency), using a physical media (cable), and light (optical fiber). All mediums are capable of multiplexing.

When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

Frequency Division Multiplexing

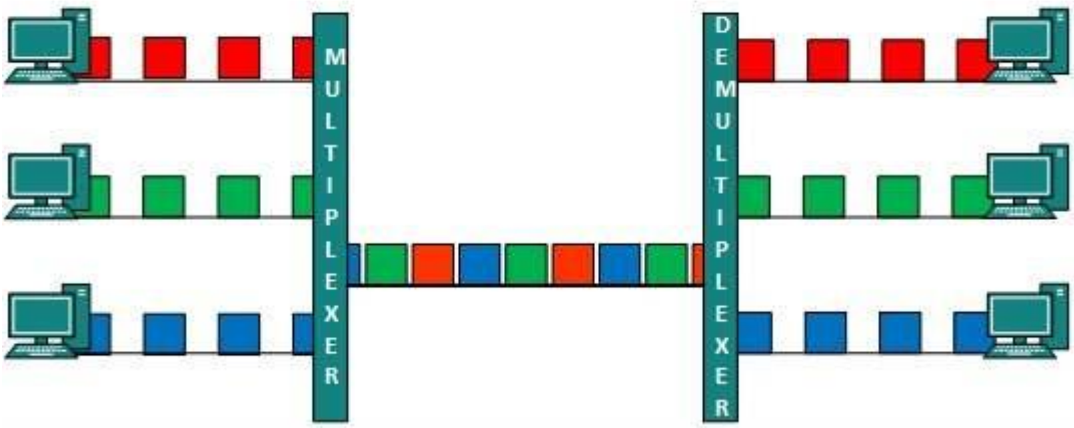
When the carrier is frequency, FDM is used. FDM is an analog technology. FDM divides the spectrum or carrier bandwidth in logical channels and allocates one user to each channel. Each user can use the channel frequency independently and has exclusive access of it. All channels are divided in such a way that they do not overlap with each other. Channels are separated by guard bands. Guard band is a frequency which is not used by either channel.



Time Division Multiplexing

TDM is applied primarily on digital signals but can be applied on analog signals as well. In TDM the shared channel is divided among its user by means of time slot. Each user can transmit data within the provided time slot only. Digital signals are divided in frames, equivalent to time slot i.e. frame of an optimal size which can be transmitted in given time slot.

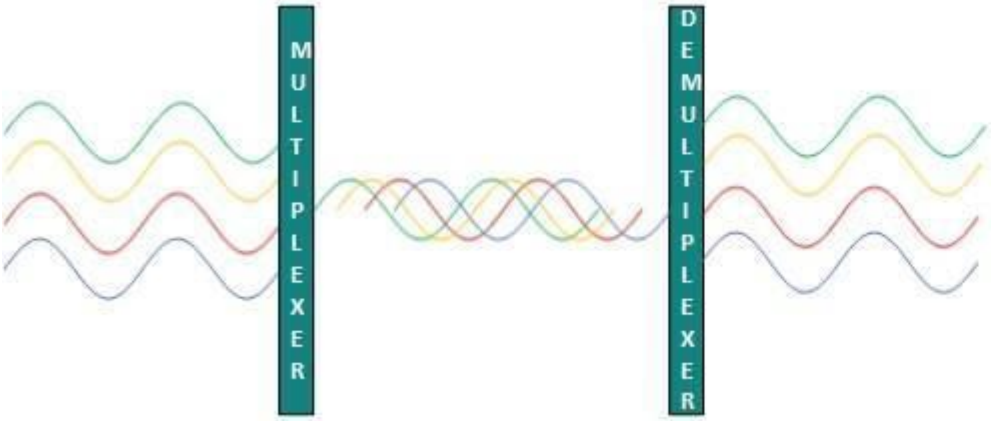
TDM works in synchronized mode. Both ends, i.e. Multiplexer and De-multiplexer are timely synchronized and both switch to next channel simultaneously.



When channel A transmits its frame at one end,the De-multiplexer provides media to channel A on the other end.As soon as the channel A’s time slot expires, this side switches to channel B. On the other end, the De-multiplexer works in a synchronized manner and provides media to channel B. Signals from different channels travel the path in interleaved manner.

Wavelength Division Multiplexing

Light has different wavelength (colors). In fiber optic mode, multiple optical carrier signals are multiplexed into an optical fiber by using different wavelengths. This is an analog multiplexing technique and is done conceptually in the same manner as FDM but uses light as signals.



Further, on each wavelength time division multiplexing can be incorporated to accommodate more data signals.

Code Division Multiplexing

Multiple data signals can be transmitted over a single frequency by using Code Division Multiplexing. FDM divides the frequency in smaller channels but CDM allows its users to full bandwidth and transmit signals all the time using a unique code. CDM uses orthogonal codes to spread signals.

Each station is assigned with a unique code, called chip. Signals travel with these codes independently, inside the whole bandwidth. The receiver knows in advance the chip code signal it has to receive.

UNIT – 6 (NETWORK ADMINISTRATION)

Cryptography and Network Security Principles

In present day scenario security of the system is the sole priority of any organization. The main aim of any organization is to protect their data from attackers. In cryptography, attacks are of two types such as Passive attacks and Active attacks.
Passive attacks are those that retrieve information from the system without affecting the system resources while active attacks are those that retrieve system information and make changes to the system resources and their operations.

The Principles of Security can be classified as follows:

1. **Confidentiality:**
   The degree of confidentiality determines the secrecy of the information. The principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.
   For example, let us consider sender A wants to share some confidential information with receiver B and the information gets intercepted by the attacker C. Now the confidential information is in the hands of an intruder C.

2. **Authentication:**
   Authentication is the mechanism to identify the user or system or the entity. It ensures the identity of the person trying to access the information. The authentication is mostly secured by using username and password. The authorized person whose identity is preregistered can prove his/her identity and can access the sensible information.

3. **Integrity:**
   Integrity gives the assurance that the information received is exact and accurate. If the content of the message is changed after the sender sends it but before reaching the intended receiver, then it is said that the integrity of the message is lost.

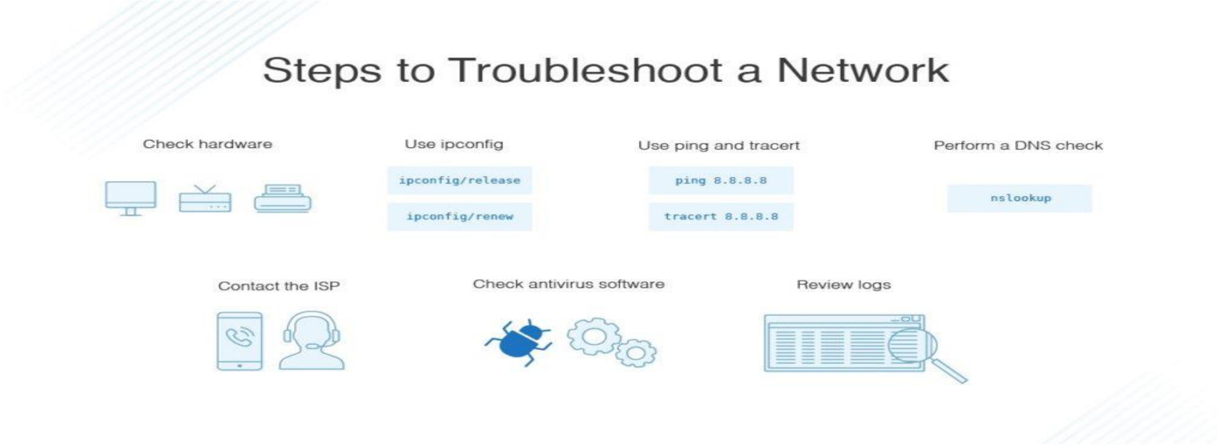
4. **Non-Repudiation:**
   Non-repudiation is a mechanism that prevents the denial of the message content sent through a network. In some cases the sender sends the message and later denies it. But the non-repudiation does not allow the sender to refuse the receiver.

5. **Access-Control:**
   The principle of access control is determined by role management and rule management. Role management determines who should access the data while rule management determines up to what extent one can access the data. The information displayed is dependent on the person who is accessing it.

6. **Availability:**
   The principle of availability states that the resources will be available to authorize party at all times. Information will not be useful if it is not available to be accessed. Systems should have sufficient availability of information to satisfy the user request.

Network Troubleshooting Process

Issues can arise at numerous points along the network. Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on. By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.



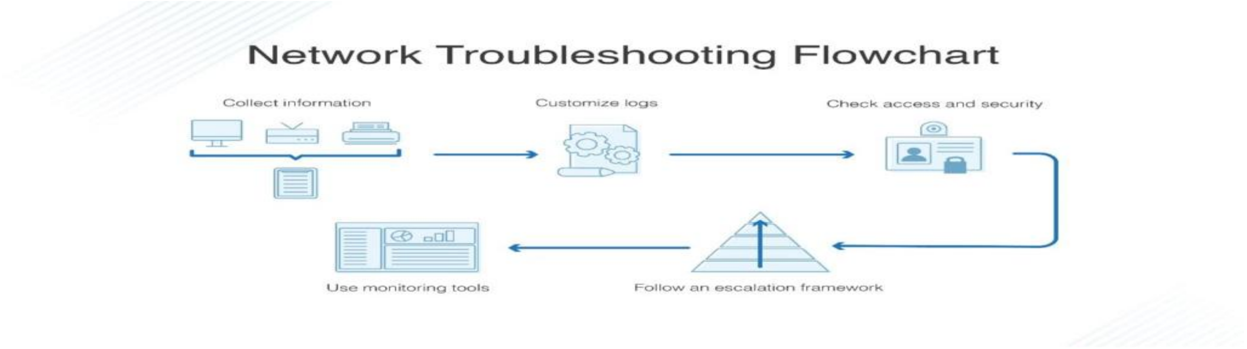
I always start troubleshooting using these simple network troubleshooting steps to help diagnose and refine the issue.

1. **Check the hardware**. When you're beginning the troubleshooting process, check all your hardware to make sure it's connected properly, turned on, and working. If a cord has come loose or somebody has switched off an important router, this could be the problem behind your networking issues. There's no point in going through the process of troubleshooting network issues if all you need to do is plug a cord in. Make sure all switches are in the correct positions and haven't been bumped accidentally. Next, turn the hardware off and back on again. This is the mainstay of IT troubleshooting, and while it might sound simplistic, often it really does solve the problem. Power cycling your modem, router, and PC can solve simple issues—just be sure to leave each device off for at least 60 seconds before you turn it back on.
2. **Use ipconfig**. Open the command prompt and type "ipconfig" (without the quotes) into the terminal. The Default Gateway (listed last) is your router's IP. Your computer's IP address is the number next to "IP Address." If your computer's IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router. Try typing in "ipconfig /release" followed by "ipconfig /renew" to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can't get a valid IP from your router, try plugging your computer straight into the modem using an ethernet cable. If it works, the problem lies with the router.
3. **Use ping and tracert**. If your router is working fine, and you have an IP address starting with something other than 169, the problems most likely located between your router and the internet. At this point, it's time to use the **ping** tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing "ping 8.8.8.8"; you can also add "-t" to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue.

   You can use the **tracert** command to do the same thing, by typing "tracert 8.8.8.8"; this will show you each step, or "hop," between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.

4. **Perform a DNS check**. Use the command "nslookup" to determine whether there's a problem with the server you're trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as "Timed Out," "Server Failure," "Refused," "No Response from Server," or "Network Is Unreachable," it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)
5. **Contact the ISP**. If all of the above turn up no problems, try contacting your internet service provider to see if they're having issues. You can also look up outage maps and related information on a Smartphone to see if others in your area are having the same problem.
6. **Check on virus and malware protection**. Next, make sure your virus and malware tools are running correctly, and they haven't flagged anything that could be affecting part of your network and stopping it from functioning.
7. **Review database logs**. Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

To make troubleshooting as efficient and painless as possible, it's also important to have some best practices in place. As you work through the steps to try to solve network issues, following these network troubleshooting best practices can help streamline the process and avoid unnecessary or redundant efforts.


Network Troubleshooting Flowchart
Collect information
Customize logs
Check access and security
Use monitoring tools
Follow an escalation framework

1. **Collect information**. To best support your end users, you first need to make sure you're clear on what the problem is. Collect enough information from both the people who are experiencing network issues and the network itself, so you can replicate or diagnose the problem. Take care not to mistake symptoms for the root cause, as what initially looks like the problem could be part of a larger issue.
2. **Customize logs**. Make sure your event and security logs are customized to provide you with information to support your troubleshooting efforts. Each log should have a clear description of which items or events are being logged, the date and time, and information on the source of the log (MAC or IP address).
3. **Check access and security**. Ensure no access or security issues have come up by checking all access permissions are as they should be, and nobody has accidentally altered a sensitive part of the network they weren't supposed to be able to touch. Check all firewalls, antivirus software, and malware software to ensure they're working correctly, and no security issues are affecting your users' ability to work.
4. **Follow an escalation framework**. There's nothing worse than going to the IT help desk and being directed to another person, who then directs you to another person, who directs you to yet another. Have a clear escalation framework of who is responsible for which issues, including the final person in the chain who can

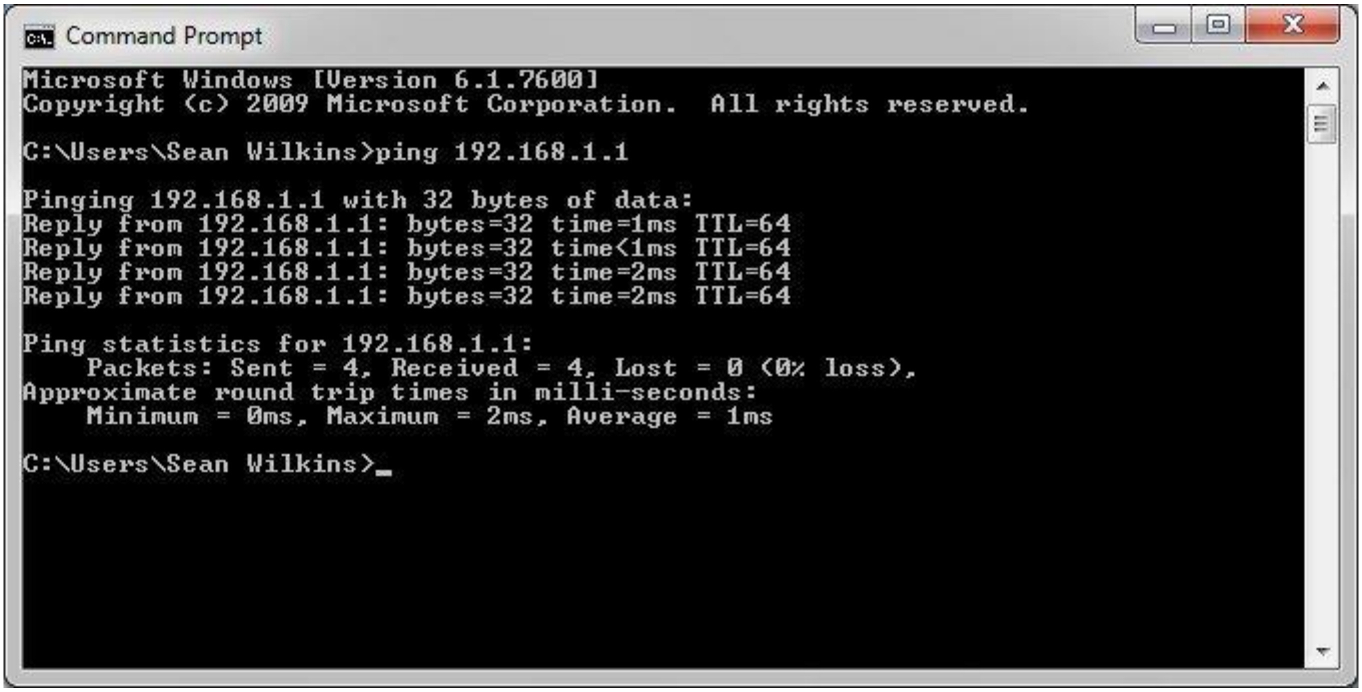
be approached for resolution. All your end users should know who they can go to about a given issue, so time isn’t wasted talking to five different people who cannot fix the problem.

5. **Use monitoring tools**. Troubleshooting can be done manually but can become time-consuming if you go through each step. When you have a bunch of people knocking on your office door or sending you frantic emails, it can be overwhelming to try to find the problem, let alone fix it. In business and enterprise situations, it’s best to use monitoring tools to make sure you’re getting all the relevant network information and aren’t missing anything vital, not to mention avoiding exposing the company to unnecessary risk.

Troubleshooting Tools

Ping

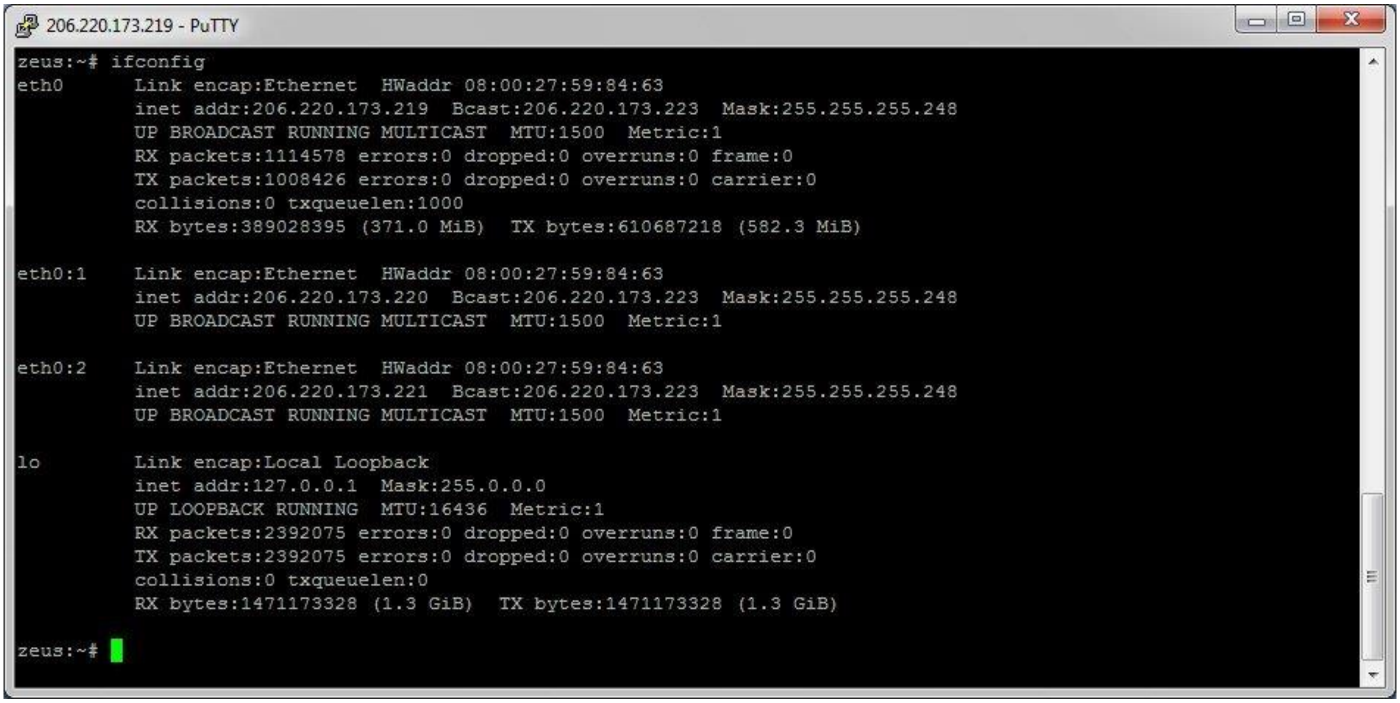
The most commonly used network tool is the ping utility. This utility is used to provide a basic connectivity test between the requesting host and a destination host. This is done by using the Internet Control Message Protocol (ICMP) which has the ability to send an echo packet to a destination host and a mechanism to listen for a response from this host. Simply stated, if the requesting host receives a response from the destination host, this host is reachable. This utility is commonly used to provide a basic picture of where a specific networking problem may exist. For example, if an Internet connection is down at an office, the ping utility can be used to figure out whether the problem exists within the office or within the network of the Internet provider. Figure below shows an example of the ping utility being used to obtain the reachability status of the locally connected router.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Sean Wilkins>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\Sean Wilkins>_
```

Ipconfig/ifconfig

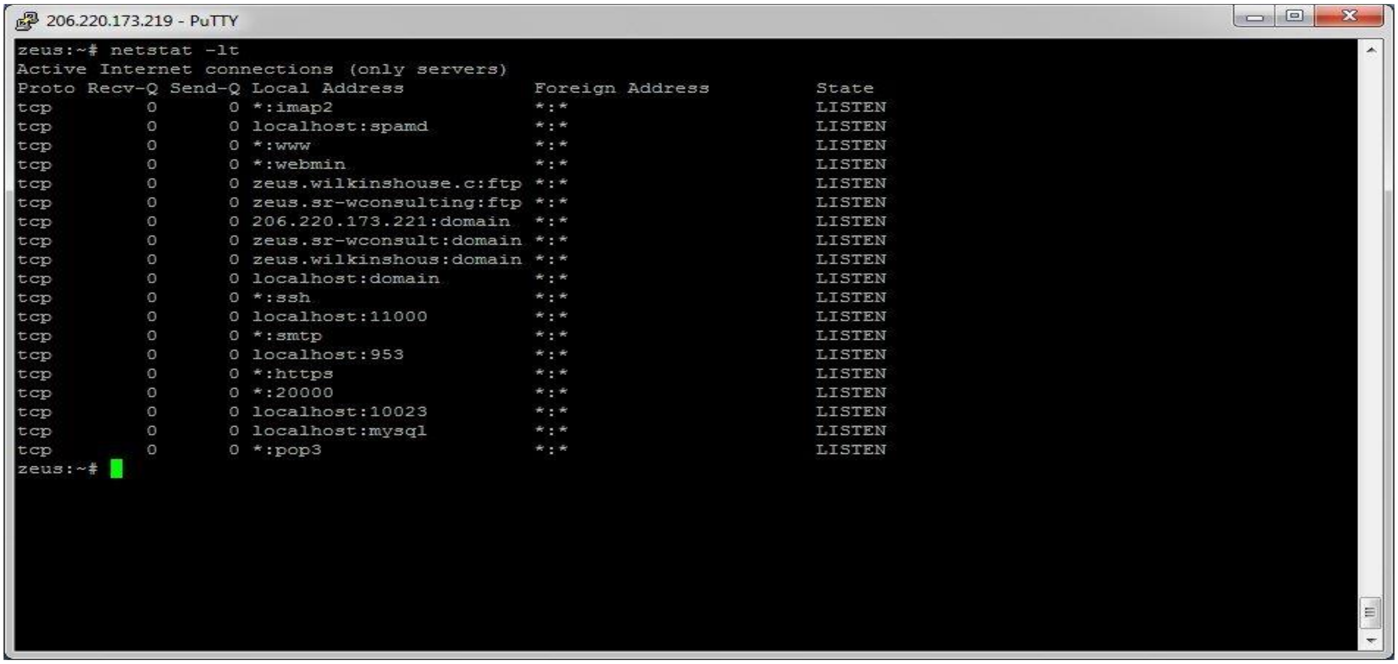
One of the most important things that must be completed when troubleshooting a networking issue is to find out the specific IP configuration of the variously affected hosts. Sometimes this information is already known when addressing is configured statically, but when a dynamic addressing method is used, the IP address of each host can potentially change often. The utilities that can be used to find out this IP configuration information include the ipconfig utility on Windows machines and the ifconfig utility on Linux/*nix based machines. Figure below shows an example of the ifconfig utility showing the IP configuration information of a queries host.



```
zeus:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:84:63
          inet addr:206.220.173.219  Bcast:206.220.173.223  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1114578 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1008426 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:389028395 (371.0 MiB)  TX bytes:610687218 (582.3 MiB)

eth0:1    Link encap:Ethernet  HWaddr 08:00:27:59:84:63
          inet addr:206.220.173.220  Bcast:206.220.173.223  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

eth0:2    Link encap:Ethernet  HWaddr 08:00:27:59:84:63
          inet addr:206.220.173.221  Bcast:206.220.173.223  Mask:255.255.255.248
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2392075 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2392075 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1471173328 (1.3 GiB)  TX bytes:1471173328 (1.3 GiB)

zeus:~#
```

Netstat

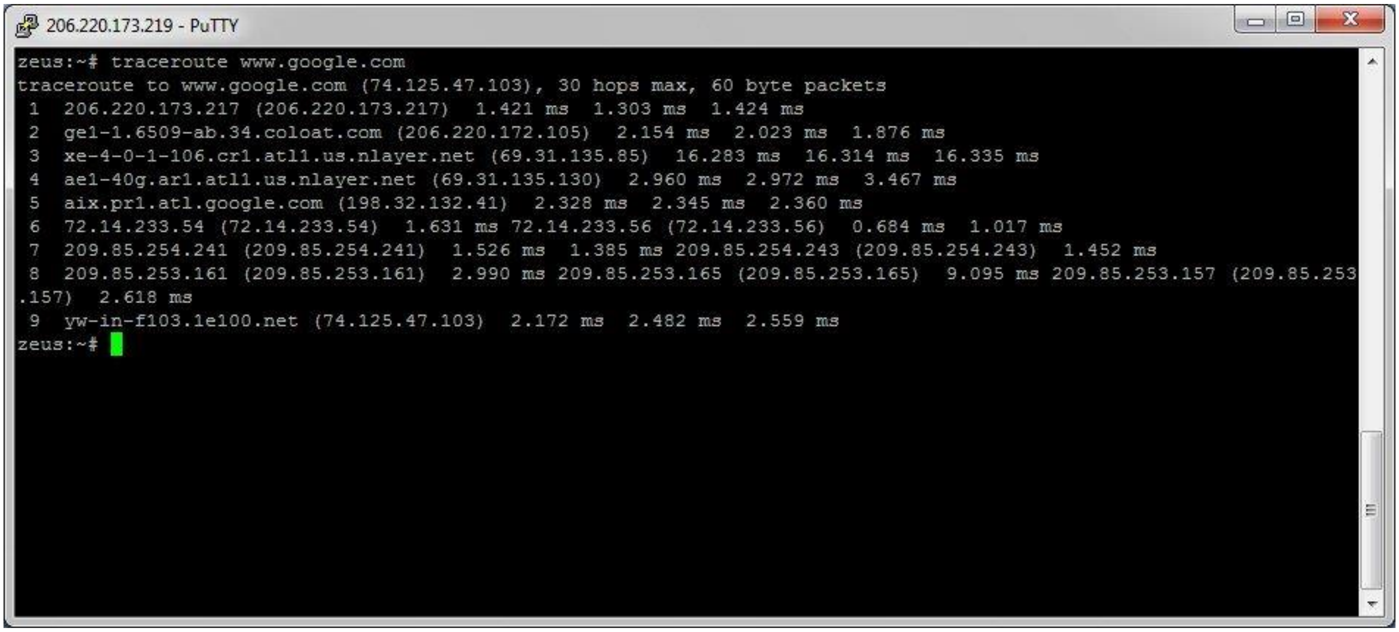
Often, one of the things that are required to be figured out is the current state of the active network connections on a host. This is very important information to find for a variety of reasons. For example, when verifying the status of a listening port on a host or to check and see what remote hosts are connected to a local host on a specific port. It is also possible to use the netstat utility to determine which services on a host that is associated with specific active ports. Figure below shows an example of the netstat utility being used to display the currently active ports on a Linux machine.



```
zeus:~# netstat -lt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 *:imap2                 *:*                     LISTEN
tcp        0      0 localhost:spamd         *:*                     LISTEN
tcp        0      0 *:www                   *:*                     LISTEN
tcp        0      0 *:webmin                *:*                     LISTEN
tcp        0      0 zeus.wilkinshouse.c:ftp *:*                     LISTEN
tcp        0      0 zeus.sr-wconsulting:ftp *:*                     LISTEN
tcp        0      0 206.220.173.221:domain  *:*                     LISTEN
tcp        0      0 zeus.sr-wconsult:domain *:*                     LISTEN
tcp        0      0 zeus.wilkinshous:domain *:*                     LISTEN
tcp        0      0 localhost:domain        *:*                     LISTEN
tcp        0      0 *:ssh                   *:*                     LISTEN
tcp        0      0 localhost:11000         *:*                     LISTEN
tcp        0      0 *:smtp                  *:*                     LISTEN
tcp        0      0 localhost:953           *:*                     LISTEN
tcp        0      0 *:https                 *:*                     LISTEN
tcp        0      0 *:20000                 *:*                     LISTEN
tcp        0      0 localhost:10023         *:*                     LISTEN
tcp        0      0 localhost:mysql         *:*                     LISTEN
tcp        0      0 *:pop3                  *:*                     LISTEN
zeus:~#
```

Tracert/traceroute

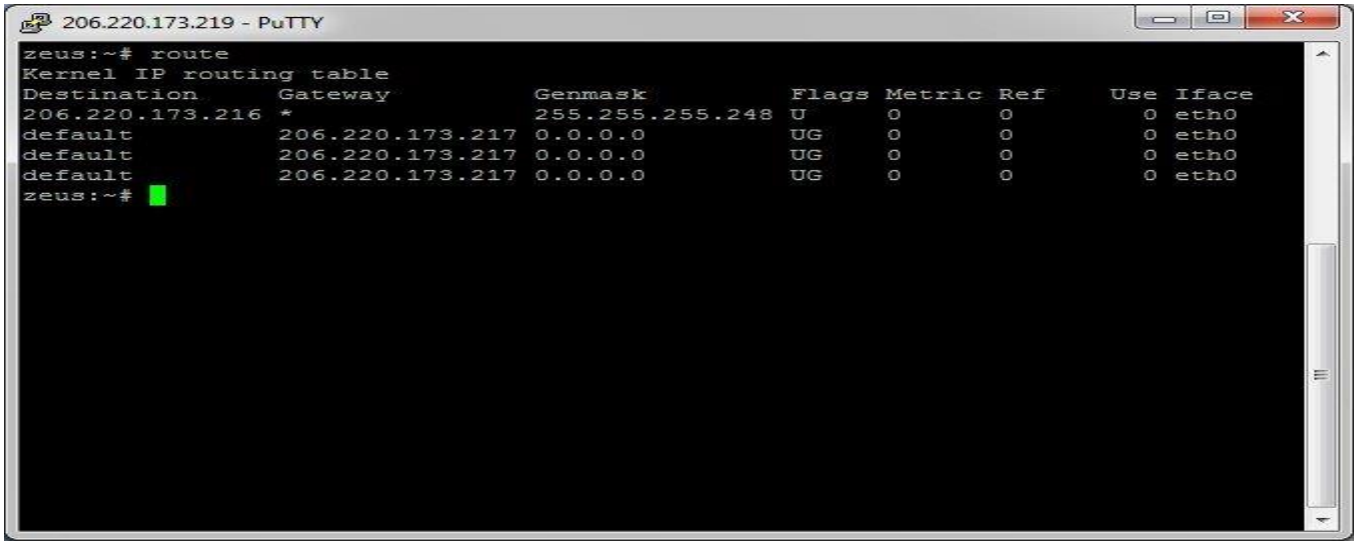
Typically, once the ping utility has been used to determine basic connectivity, the tracert/traceroute utility can used to determine more specific information about the path to the destination host including the route the packet takes and the response time of these intermediate hosts. Figure 2 below shows an example of the tracert utility being used to find the path from a host inside an office to www.google.com. The tracert utility and traceroute utilities perform the same function but operate on different operating systems, Tracert for Windows machines and traceroute for Linux/*nix based machines.



```
zeus:~# traceroute www.google.com
traceroute to www.google.com (74.125.47.103), 30 hops max, 60 byte packets
 1  206.220.173.217 (206.220.173.217)  1.421 ms  1.303 ms  1.424 ms
 2  ge1-1.6509-ab.34.coloat.com (206.220.172.105)  2.154 ms  2.023 ms  1.876 ms
 3  xe-4-0-1-106.cr1.atl1.us.nlayer.net (69.31.135.85)  16.283 ms  16.314 ms  16.335 ms
 4  ae1-40g.ar1.atl1.us.nlayer.net (69.31.135.130)  2.960 ms  2.972 ms  3.467 ms
 5  aix.pr1.atl.google.com (198.32.132.41)  2.328 ms  2.345 ms  2.360 ms
 6  72.14.233.54 (72.14.233.54)  1.631 ms 72.14.233.56 (72.14.233.56)  0.684 ms  1.017 ms
 7  209.85.254.241 (209.85.254.241)  1.526 ms  1.385 ms 209.85.254.243 (209.85.254.243)  1.452 ms
 8  209.85.253.161 (209.85.253.161)  2.990 ms 209.85.253.165 (209.85.253.165)  9.095 ms 209.85.253.157 (209.85.253
.157)  2.618 ms
 9  yw-in-f103.1e100.net (74.125.47.103)  2.172 ms  2.482 ms  2.559 ms
zeus:~# 
```

Route

The last of the tools covered in this article is the route utility. This utility is used to display the current status of the routing table on a host. While the use of the route utility is limited in common situations where the host only has a single IP address with a single gateway, it is vital in other situations where multiple IP address and multiple gateways are available. Figure 13 below shows an example of the route utility being used on a Windows machine.



```
zeus:~# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
206.220.173.216 *               255.255.255.248 U     0      0        0 eth0
default         206.220.173.217 0.0.0.0         UG    0      0        0 eth0
default         206.220.173.217 0.0.0.0         UG    0      0        0 eth0
default         206.220.173.217 0.0.0.0         UG    0      0        0 eth0
zeus:~# 
```

Wireshark

Wireshark is a protocol analyzer and one of the go-to networking tools for organizations of all sizes when network issues need to be troubleshot with a high level of granularity. The benefit of using Wireshark to analyze network traffic is that you will be able to view the raw network packets, and this will often allow you to identify the root cause of an issue. This can be especially helpful in situations where it is unclear which application is not doing what it is supposed to or when you try to reverse engineer the functionality of a poorly-documented program.

The tradeoff here is that you will have a lot of data to parse through, so some technical knowledge may be required to drill down and identify the important information.

Key Features:

- Packet capture
- Protocol analyzer
- Free to use

Nmap

Nmap is a popular security auditing and network exploration tool released under a custom open source license based on GPLv2. While the most popular use cases for nmap are security scans and penetration testing, it can prove quite helpful as a network troubleshooting tool as well. For example, if you are dealing with an unfamiliar app and want to find out what services are running and which ports are open, nmap can help. Nmap itself uses a command-line interface (CLI), but that doesn't mean you are out of luck if you prefer a graphical user interface (GUI). Zenmap is the official nmap GUI and is a good way for beginners to start working with nmap.

Key Features:

- Command-line utility
- Network troubleshooter
- Free to use

TCPDUMP

Tcpdump is a type of packet analyzer software utility that monitors and logs TCP/IP traffic passing between a network and the computer on which it is executed.

Tcpdump is an open-source network utility that is freely available under the BSD license. Tcpdump works on the command line interface and provides descriptions of packet content in several formats, depending on the command used.

Tcpdump is primarily a network monitoring and management utility that captures and records TCP/IP data on the run time. Tcpdump is designed to provide statistics about the number of packets received and captured at the operating node for network performance analysis, debugging and diagnosing network bottlenecks and other network oriented tasks.

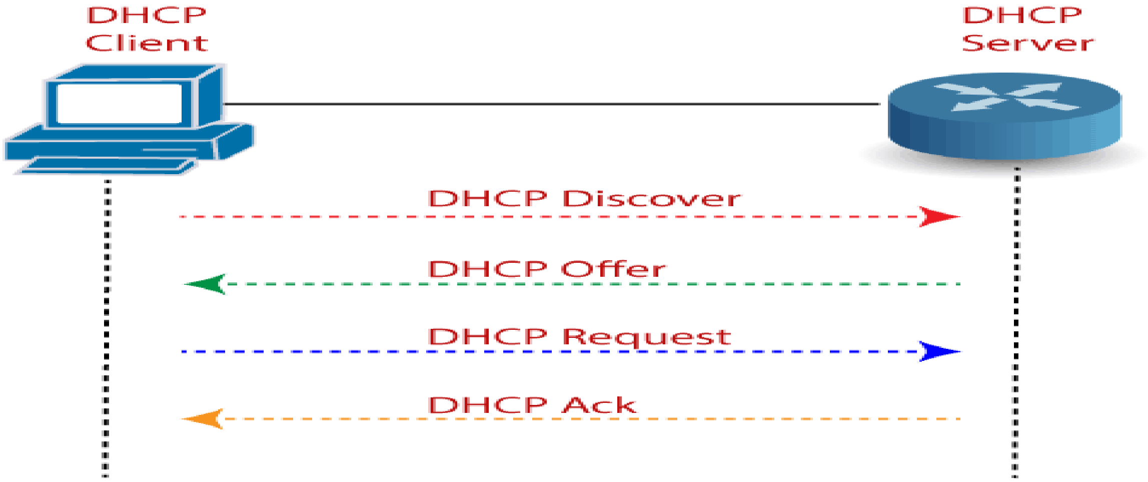
Because it is a command line utility, data retrieved through tcpdump can vary. For example, when used with -An operator, it prints out each packet in ASCII format. Tcpdump is supported by most Unix-based operating systems, such as Linux, Mac OSX and BSD. The Windows variant of tcpdump is known as WinDump.

DHCP (Dynamic Host Configuration Protocol) Server

- DHCP stands for **Dynamic Host Configuration Protocol**.
- It is a client server-based architecture which involves DHCP client and DHCP server.
- It is a **messaging system** for the communication between **the DHCP server** and **DHCP client**.
- It allows the clients to acquire their IP address dynamically.
- DHCP uses UDP port numbers **67** for destination server **and** port number **68** for the client.

The DHCP messaging system’s message and their types are given below:

- Discover
- Offer
- Request
- Acknowledgment



DHCP MESSAGE

Every DHCP server that receives the message responds with a DHCP offer containing:

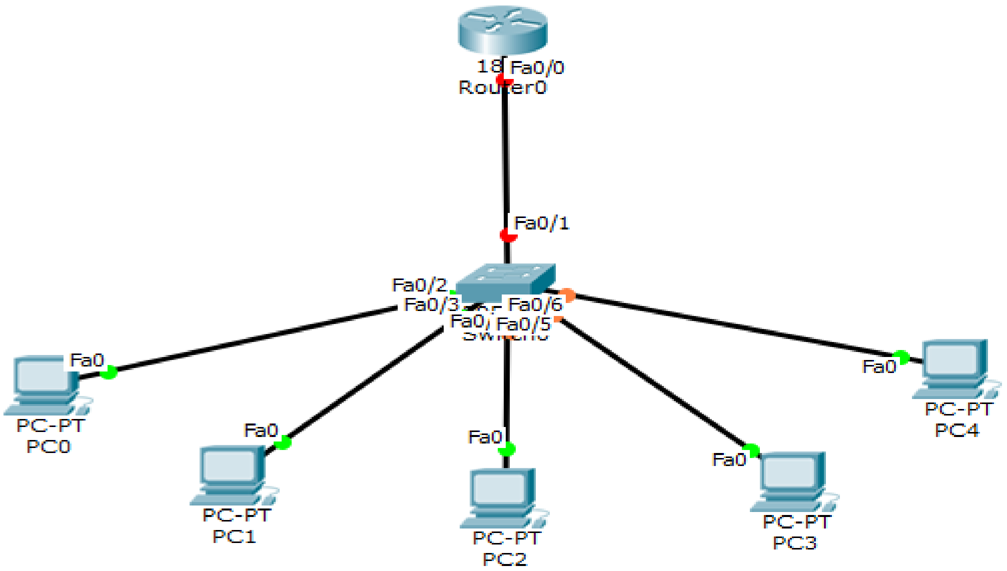
- The IP Address being offered to the DHCP client.
- The network mask offered to the DHCP client.
- The amount of time the client can keep and use this address.
- The IP address of the DHCP server makes this offer.

Components of DHCP

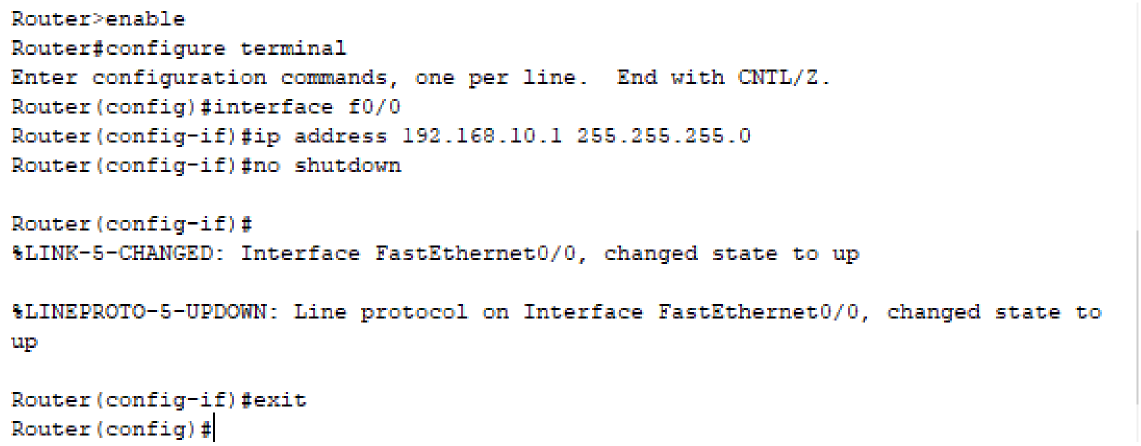
Before start configuring DHCP, it is important to understand all of its components.
A list of DHCP components are given below:
DHCP Server: DHCP Server is a networked device that is used to run the DHCP service and hold the information about the IP address or related configuration.
DHCP Client: DHCP client receives configuration information from a DHCP Server. It can be a computer, mobile phone, or any other device that requires connectivity to the network.
IP address pool: IP address pool is the range of IP addresses that are available to DHCP clients. These addresses are generally handed out sequentially from lowest to highest.

Subnet: Subnet helps us to keep networks manageable.
DHCP relay: DHCP relay is responsible for forwarding the requests and responses between the DHCP clients and the DHCP servers.

Configure DHCP
There are following steps involve configuring DHCP on a Router –
Step1: Create the Network topology:



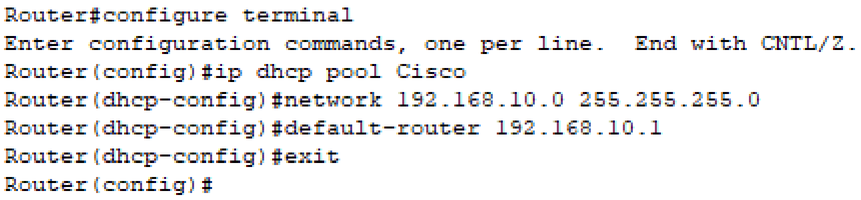
Step2: On the router0, configure an IP address to the router’s interface that is connected to the switch and act as the default gateway.



```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#exit
Router(config)#
```

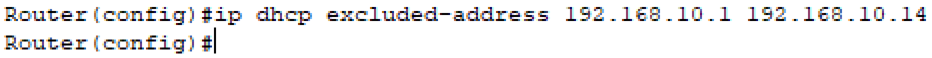
Step3: Now, create an **ip dhcp pool** and named it as **Cisco**. In this Pool, provide a **Network address** that has given to the **DHCP clients**.

After creating the DHCP pool, assign the router's interface ip address as a default-router address for clients.



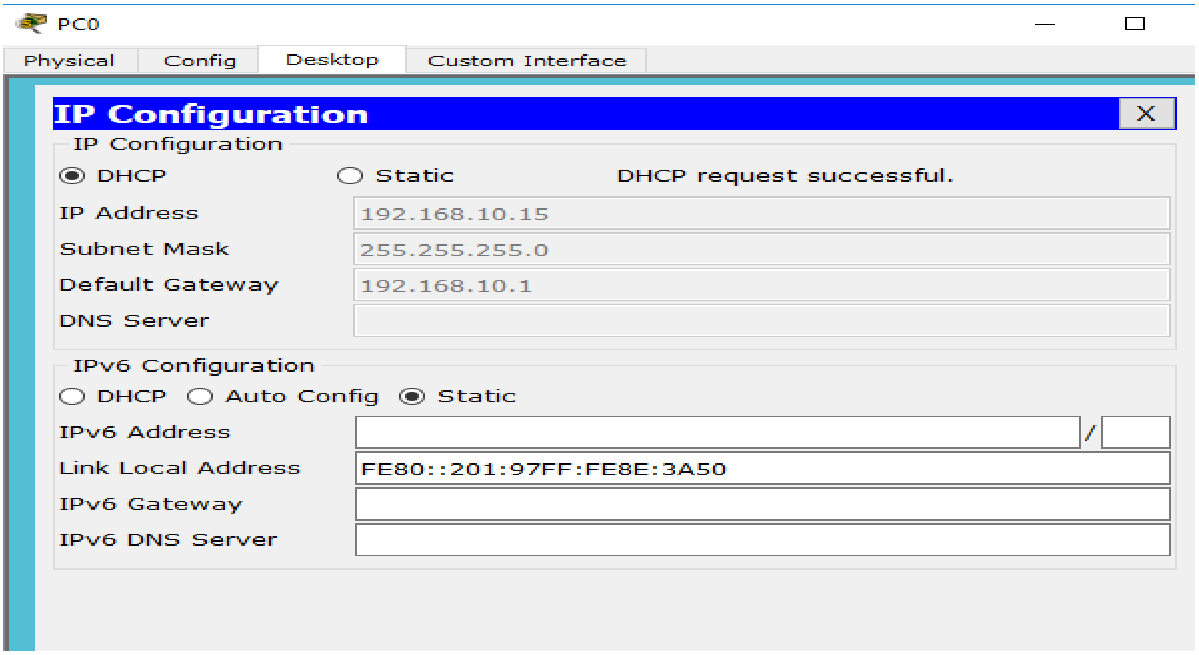
```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip dhcp pool Cisco
Router(dhcp-config)#network 192.168.10.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.10.1
Router(dhcp-config)#exit
Router(config)#
```

Step4: In this step, we will exclude ip address range by typing **"ipdhcp excluded address"** command.



```
Router(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.14
Router(config)#
```

After completing all the above steps, click on any PC then go to Desktop -> IP Configuration ->DHCP.



IP Configuration

IP Configuration

● DHCP ○ Static DHCP request successful.

IP Address 192.168.10.15

Subnet Mask 255.255.255.0

Default Gateway 192.168.10.1

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::201:97FF:FE8E:3A50

IPv6 Gateway

IPv6 DNS Server

You see that the ip address 192.168.10.15 is configured automatically, as it is shown in the above screenshot.

Advantages of DHCP

DHCP offers the following advantages:

- **IP address management –**DHCP provides easier IP address management scheme. In a network, without DHCP, you must assign IP addresses manually. But When the DHCP is enabled, the DHCP server provides IP address automatically.
- **Centralized network client configuration –** In the DHCP, all configuration information is stored in one place that is**"DHCP data store."** It does not need a client to change the configuration. It can make changes for multiple clients just by changing the information stored in the data store.

- **Support of local clients and remote client –** DHCP supports both local clients and remote client by providing the IP addresses automatically to each client that work on a network.
- **Large network support –**There are millions of clients that can use DHCP. The DHCP uses multithreading to process the clients request simultaneously.
- **Remove Delicacy –** DHCP removes duplicate or invalid assignment of IP addresses. Therefore, no chance of conflicts in IP addresses.

Disadvantages of DHCP

- **Makes router busy –** When we configure DHCP on a router, it will make the router busier and consume some additional memory.
- **Security Issues –** In DHCP, there is a high-security risk. Because the information is sent over the network, that's why there may be a chance of information getting lost or hacked by someone.
- The client is not able to access the network in the absence of a DHCP server.

Workgroup/Domain Networking

Domain:

Domain is a client/server network where user can login from any device of the office. Also known as Remote login. It has a centralized administration and all devices can be managed from a centralized device. It prefers a centralized storage and all the users data is stored at a centralized storage device which can be NAS or SAN.

Workgroup:

Workgroup is a peer to peer windows computer network, where users can use his login credentials only on his or her system and not others. It holds a distributed administration wherein each user can manage his machine independently. Most storage is distributed. Each device has its own dedicated storage.

Difference between Domain and Workgroup

S.No.	Domain	Workgroup
1	The computers in a domain have a centralized database.	The computers in workgroup mainly have its own local database.
2	A domain is mainly to transfer and share sensitive and important data only.	A Workgroup is used to share less secure and personal data only due to less security.
3	A domain is mainly preferred for large public and business networks.	A workgroup is mainly preferred for small local area networks like schools, colleges, buildings, etc.
4	A domain is used to transfer and share sensitive and important data due to security.	A workgroup is used to share personal data as it is less secure.
5	A domain can work better for large numbers of devices.	A workgroup works better for fewer computers.
6	The domain names are provided by domain controller on the basis of IP address.	In workgroup there are no dependencies on any hardware components and server for assigning the name.
7	Data can be recovered in a domain from the centralized storage.	Data recovery is not possible in a workgroup due to the local storage of each device.
8	A Domain can be formed using the devices of one or more different networks domain and adding all the intended devices to it.	The devices of the same network can only be added to a workgroup.

UNIT – 7 (Introduction to Wireless Networks)

Wireless LAN stands for **Wireless Local Area Network**. It is also called LAWN (**Local Area Wireless Network**). WLAN is one in which a mobile user can connect to a Local Area Network (LAN) through a wireless connection.

The IEEE 802.11 group of standards defines the technologies for wireless LANs. For path sharing, 802.11 standard uses the Ethernet protocol and CSMA/CA (carrier sense multiple access with collision avoidance). It also uses an encryption method i.e. wired equivalent privacy algorithm.

Wireless LANs provide high speed data communication in small areas such as building or an office. WLANs allow users to move around in a confined area while they are still connected to the network.

In some instance wireless LAN technology is used to save costs and avoid laying cable, while in other cases, it is the only option for providing high-speed internet access to the public. Whatever the reason, wireless solutions are popping up everywhere.

Examples of WLANs that are available today are NCR's waveLAN and Motorola's ALTAIR.

Advantages of WLANs

- **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
- **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.
- **Design:** Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.
- **Robustness:** Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- **Cost:** The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons. First, after providing wireless access to the wireless network via an access point for the first user, adding additional users to a network will not increase the cost. And second, wireless LAN eliminates the direct costs of cabling and the labor associated with installing and repairing it.
- **Ease of Use:** Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

Disadvantages of WLANs

- **Quality of Services:** Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
- **Proprietary Solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
- **Restrictions:** Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.

- **Global operation:** Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
- **Low Power:** Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
- **License free operation:** LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
- **Robust transmission technology:** If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.).Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

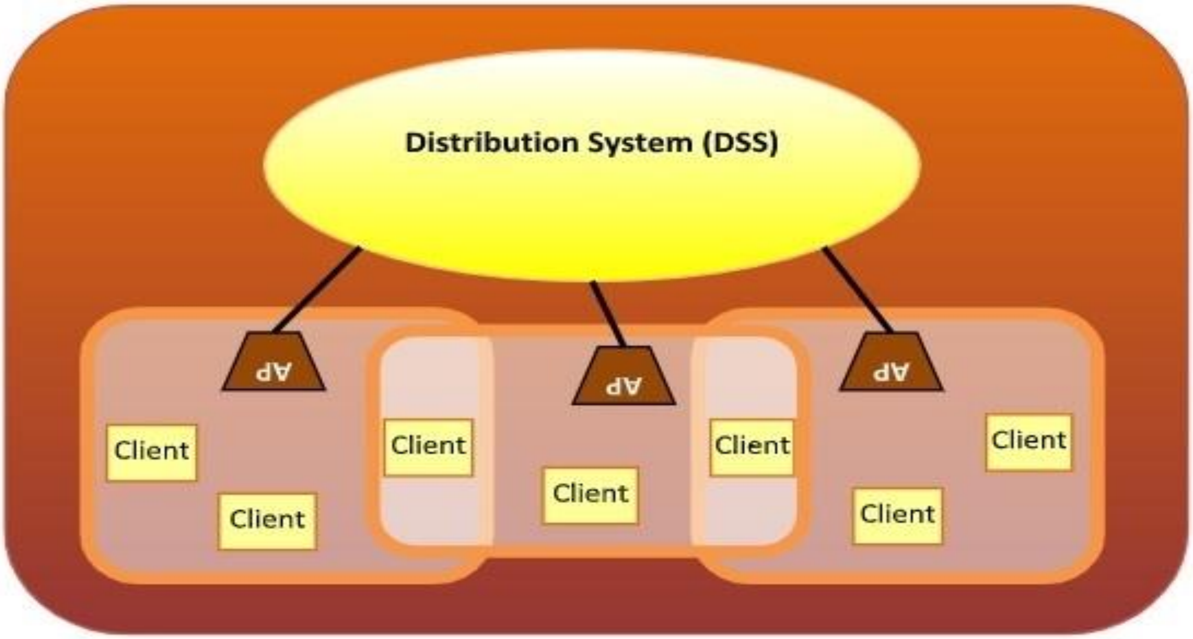
Wireless LAN Protocols

Wireless LANs refer to LANs (Local Area Networks) that use high frequency radio waves instead of cables for connecting the devices. It can be conceived as a set of laptops and other wireless devices communicating by radio signals. Users connected by WLANs can move around within the area of network coverage. Most WLANs are based upon the standard IEEE 802.11 or WiFi.

Configuration of Wireless LANs

Each station in a Wireless LAN has a wireless network interface controller. A station can be of two categories −

- **Wireless Access Point (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access points. The APs are wired together using fiber or copper wires, through the distribution system.
- **Client** − Clients are workstations, computers, laptops, printers, smart phones etc. They are around tens of metres within the range of an AP.



Types of WLAN Protocols

IEEE 802.11 or WiFi has a number of variations, the main among which are −

- **802.11a Protocol**− This protocol supports very high transmission speeds of 54Mbps. It has a high frequency of 5GHz range, due to which signals have difficulty in penetrating walls and other obstructions. It employs Orthogonal Frequency Division Multiplexing (OFDM).

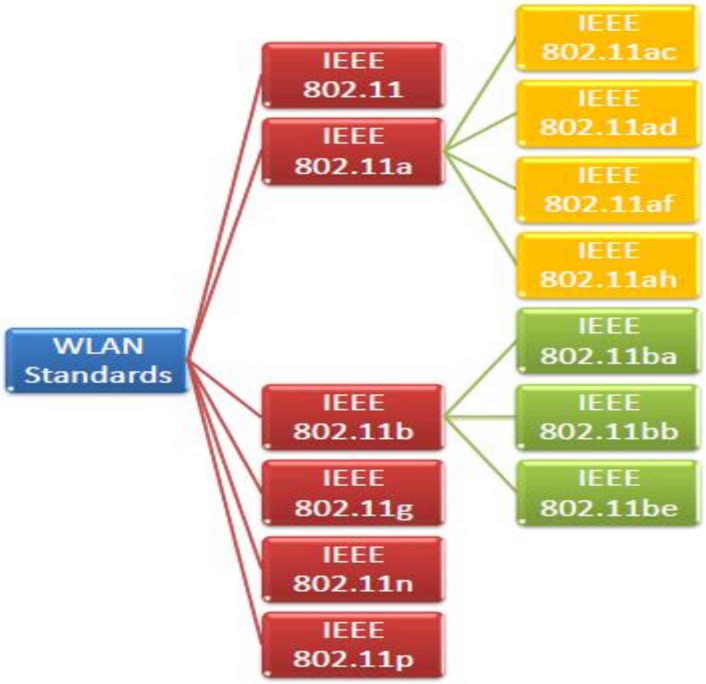
- **802.11b Protocol** − This protocol operates within the frequency range of 2.4GHz and supports 11Mbps speed. It facilitates path sharing and is less vulnerable to obstructions. It uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with Ethernet protocol.

- **802.11g Protocol** − This protocol combines the features of 802.11a and 802.11b protocols. It supports both the frequency ranges 5GHz (as in 802.11a standard) and 2.4GHz (as in 802.11b standard). Owing to its dual features, 802.11g is backward compatible with 802.11b devices. 802.11g provides high speeds, varying signal range, and resilience to obstruction. However, it is more expensive for implementation.

- **802.11n Protocol** − Popularly known as Wireless N, this is an upgraded version of 802.11g. It provides very high bandwidth up to 600Mbps and provides signal coverage. It uses Multiple Input/Multiple Output (MIMO), having multiple antennas at both the transmitter end and receiver ends. In case of signal obstructions, alternative routes are used. However, the implementation is highly expensive.

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high frequency radio waves for connecting the nodes.

There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p. All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA). Also, they have support for both centralized base station based as well as ad hoc networks.



IEEE 802.11

IEEE 802.11 was the original version released in 1997. It provided 1 Mbps or 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.

IEEE 802.11a

802.11a was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11. It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code. As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.

Further amendments to 802.11a are 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

IEEE 802.11b

802.11b is a direct extension of the original 802.11 standard that appeared in early 2000. It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band. It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs. However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.

Further amendments to 802.11b are 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be.

IEEE 802.11g

802.11g was indorsed in 2003. It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a). It is fully backward compatible with 802.11b. 802.11g devices also faces interference from other devices operating in 2.4 GHz band.

IEEE 802.11n

802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands. It has variable data rate ranging from 54 Mbps to 600 Mbps. It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).

IEEE 802.11p

802.11 is an amendment for including wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS). They include network communications between vehicles moving at high speed and the environment. They have a data rate of 27 Mbps and operate in 5.9 GHz band.

IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

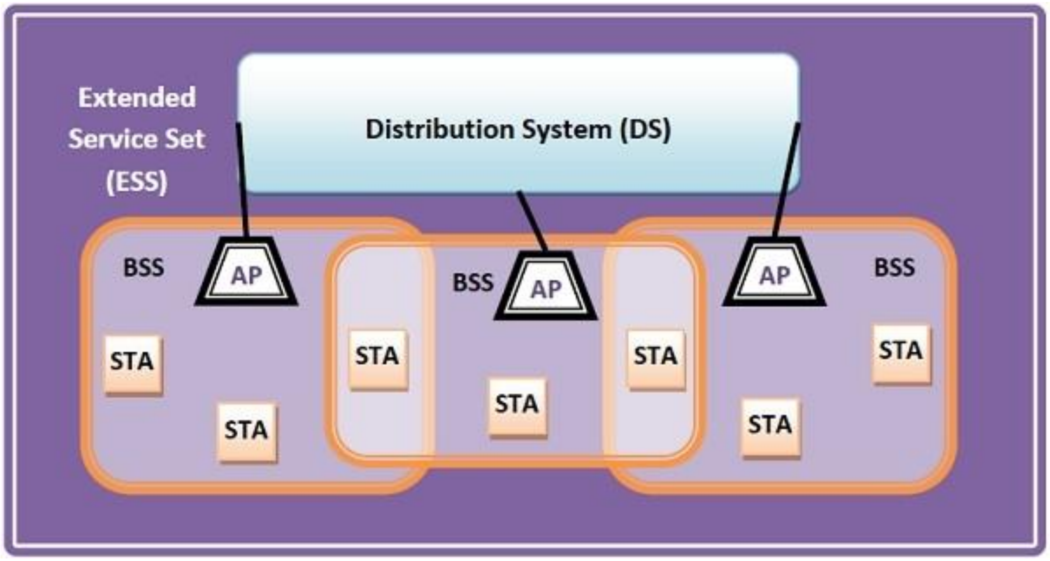
IEEE 802.11 Architecture

The components of an IEEE 802.11 architecture are as follows −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
    - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.

    - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.

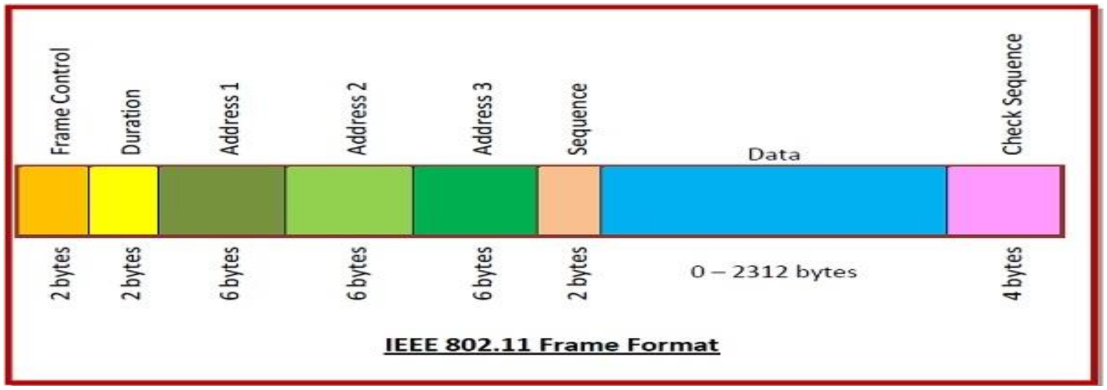
- Each station has a wireless network interface controller.
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation−
    - Infrastructure BSS − Here, the devices communicate with other devices through access points.
    - Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.



Frame Format of IEEE 802.11

The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are −

- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields** − There are three 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.



IEEE 802.11 Frame Format

Compare LiFi, WiFi, Wimax and Bluetooth

Features	Li-Fi	Wi-Fi	WiMAX	Bluetooth
Full form	Li-Fi (Light Fidelity)	Wi-Fi (Wireless Fidelity)	WiMAX (Worldwide Interoperability for Microwave Access)	Bluetooth Full From the epithet of the tenth-century king Harald "Bluetooth" Gormsson.
Operation	Li-Fi transmits data using light with the help of LED bulbs.	WiFi transmits data using radio waves with the help of Wi-Fi router.	Broadband Wireless Access.	Anywhere at least two Bluetooth devices exist.
Interference	Do not have any interference issues similar to radio frequency waves.	Will have interference issues from nearby access points (routers).	WiMAX communications pose a significant interference threat to satellite signals transmitted in the C-band frequency.	Bluetooth devices interfere with other technologies.
Technology	Present IrDA compliant devices	WLAN802.11a/b/g/n/ac/ad standard compliant devices	Wireless metropolitan area network (WMAN)	WPAN
Applications	Used in airlines, undersea explorations, operation theaters in the hospitals, office and home premises for data transfer and internet browsing	Used for internet browsing with the help of wifi kiosks or Wi-Fi hotspots	WiMAX serves a larger interoperable network.	Bluetooth applications is huge, because we transact business and communicate more with people who are close by than with those who are far away.
Merits	Interference is less, can pass through salty sea water, works in a densy region.	Interference is more, cannot pass through sea water, works in less densy region.	WiMAX can be used for long ranges. It provides broadband connectivity up to varied ranges, around 30 km.	Setting up a Bluetooth connection between two devices is quick and easy. A Bluetooth headset is compatible with any other device that supports Bluetooth,
Privacy	In Li-Fi, light is blocked by the walls and hence will provide more secure data transfer	In WiFi, RF signal can not be blocked by the walls and hence need to employ techniques to achieve secure data transfer.	WiMAX uses X.509 or PKMv2 as authentication algorithms. Mandatory-3DES Optional- AES	Bluetooth offers several security modes, and device manufacturers determine which mode to include in a Bluetooth-enabled gadget.
Data transfer speed	About 1 Gbps	WLAN-11n offers 150Mbps, About 1-2 Gbps can be achieved using WiGig/Giga-IR	Works at 5 bps/Hz and can peak up to 100 Mbps in a 20 MHz channel.	800KBps
Frequency of operation	10 thousand times frequency spectrum of the radio	2.4GHz, 4.9GHz and 5GHz	Licensed/Unlicensed 2 G to 11 GHz	2.4GHz
Data density	Works in high dense environment	Works in less dense environment due to interference related issues	Works in high dense environment	Less dense
Coverage distance	About 10 meters	About 32 meters (WLAN 802.11b/11g), vary based on transmit power and antenna type	Up to 40 miles	About 10 meters
System components	Lamp driver, LED bulb (lamp) and photo detector will make up complete Li-Fi system.	Requires routers to be installed, subscriber devices (laptops, PDAs, desktops) are referred as stations	There are three main components of WiMax network architecture. He first component is the mobile stations, second network is an access service network and third component is connectivity service network which is responsible for providing IP functions.	Four major components: Radio Unit(radio transceiver) Baseband Unit (flash memory & CPU) Software Stack (driver software) Application Software (user interface)
Power consumption	Medium	Medium	High	Low
Cost price	Low	Medium	Medium	Low
Working Concept	Direct Binary Data Serving	Various Topologies	Request/Grant	Master- Slave

Wireless Security

Wireless security is nothing but protecting computers, smartphones, tablets, laptops and other portable devices along with the networks they are connected to, from threats and vulnerabilities associated with wireless computing. This is an introductory tutorial that covers the basics of Wireless Security and how to deal with its various modules and sub-modules.

In this tutorial, you will be taken on a journey through different methods of wireless communication. You will learn about **Wireless Local Area Network** (WLAN) as most of us know it, and then go deeper into the practical aspects behind wireless security. You will be amazed at how easy it is to collect a lot of sensitive information about wireless network and the data flowing through it, using basic tools that are easily available for anyone who knows how to use it.

Before we go deeper into the "**hacking**" side of the wireless communication, you will need to go through a plethora of theoretical concepts and diagrams of normal wireless system operation. Nevertheless, theoretical content will be kept to absolutely minimum throughout this Tutorial - it is the practical side of the things that is most encouraging and the most enjoyable part for everyone!

When we think about wireless communication, we imagine some systems connected to antennas that speak together over the air using radio waves that are invisible to human eye. Honestly speaking, this is perfectly a true definition, but in order to break things (or rather you prefer the word "hack") you need to learn how all those concepts and architectures work together.

Wireless Terminologies

First, let's go through the bunch of basic terms, related to wireless communication. Progressively, we will get into more advanced stuff going all along this path together.

Wireless Communication

Wireless communication refers to any type of data exchange between the parties that is performed wirelessly (over the air). This definition is extremely wide, since it may correspond to many types of wireless technologies, like −

- Wi-Fi Network Communication
- Bluetooth Communication
- Satellite Communication
- Mobile Communication

All the technologies mentioned above use different communication architecture, however they all share the same "Wireless Medium" capability.

Wi-Fi

Wireless Fidelity (Wi-Fi) refers to wireless local area network, as we all know them. It is based on **IEEE 802.11** standard. Wi-Fi is a type of wireless network you meet almost everywhere, at your home, workplace, in hotels, restaurants and even in taxis, trains or planes. These 802.11 communication standards operate on either **2.4 GHz or 5 GHz ISM radio bands**.

These devices are easily available in the shops that are compatible with Wi-Fi standard, they have following image visible on the device itself. I bet you have seen it hundreds of times in various shops or other public places!

Wireless Clients

Wireless clients are considered to be any end-devices with a wireless card or wireless adapter installed. Now, in this 21st century, those devices can be almost anything −

- **Modern Smartphones** − These are one of the most universally used wireless devices you see in the market. They support multiple wireless standards on one box, for example, Bluetooth, Wi-Fi, GSM.
- **Laptops** − These are a type of device which we all use every single day!
- **Smartwatch** − An example of Sony based smartwatch is shown here. It can synchronize with your smartphone via a Bluetooth.
- **Smart-home Equipment** − With the current progress of the technology, smart-home equipment might be for example a freezer that you can control over Wi-Fi or a temperature controller.

The list of possible client devices is growing every single day. It sounds a little scary that all of those devices/utilities we use on a daily basis can be controlled via a wireless network so easily. But at the same time, remember that all the communication flowing through a wireless medium can be intercepted by anyone who is just standing at the right place at the right time.

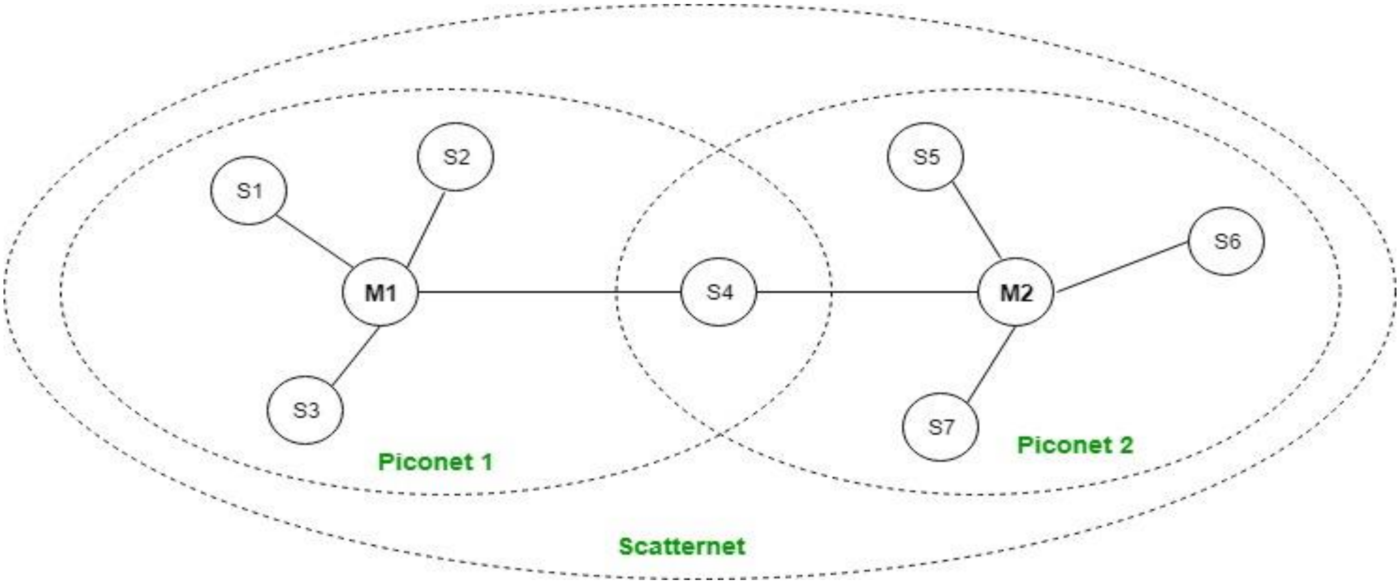
Bluetooth

It is a Wireless Personal Area Network (WPAN) technology and is used for exchanging data over smaller distances. This technology was invented by Ericson in 1994. It operates in the unlicensed, industrial, scientific and medical (ISM) band at 2.4 GHz to 2.485 GHz. Maximum devices that can be connected at the same time are 7. Bluetooth ranges upto 10 meters. It provides data rates upto 1 Mbps or 3 Mbps depending upon the version. The spreading technique which it uses is FHSS (Frequency hopping spread spectrum). A bluetooth network is called **piconet** and a collection of interconnected piconets is called **scatternet**.

Bluetooth Architecture:

The architecture of bluetooth defines two types of networks:

1. Piconet
2. Scatternet



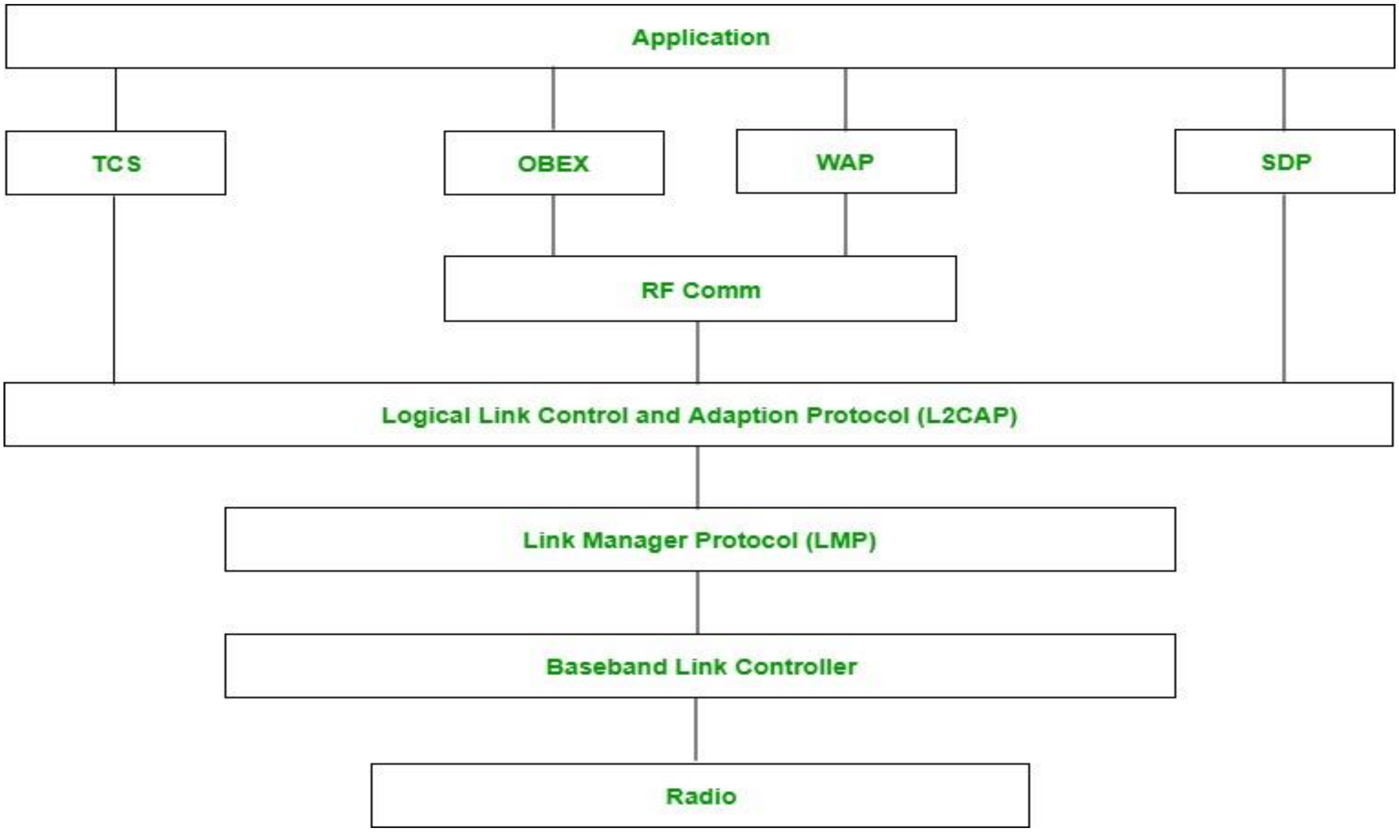
Piconet

Piconet is a type of bluetooth network that contains **one primary node** called master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there are total of 8 active nodes which are present at a distance of 10 metres. The communication between the primary and secondary node can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also have **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it get converted to the active state.

Scatternet

It is formed by using **various piconets**. A slave that is present in one piconet can be act as master or we can say primary in other piconet. This kind of node can receive message from master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave. This type of node is refer as bridge node. A station cannot be master in two piconets.

Bluetooth protocols stack:


Application
TCS
OBEX
WAP
SDP
RF Comm
Logical Link Control and Adaption Protocol (L2CAP)
Link Manager Protocol (LMP)
Baseband Link Controller
Radio

1. Radio (RF) Layer:
It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of bluetooth transceiver. It defines two types of physical link: connection-less and connection-oriented.

2. Baseband Link Layer:
It performs the connection establishment within a piconet.

3. Link Manager Protocol Layer:
It performs the management of the already established links. It also includes authentication and encryption processes.

4. Logical Link Control and Adaption Protocol Layer:
It is also known as the heart of the bluetooth protocol stack. It allows the communication between upper and lower layers of the bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs the segmentation and multiplexing.

5. SDP Layer:
It is short for Service Discovery Protocol. It allows to discover the services available on another bluetooth enabled device.

6. RF comm Layer:
It is short for Radio Frontend Component. It provides serial interface with WAP and OBEX.

7. OBEX:
It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

8. WAP:
It is short for Wireless Access Protocol. It is used for internet access.

9. TCS:
It is short for Telephony Control Protocol. It provides telephony service.
10. Application Layer
It enables the user to interact with the application.

Advantages:

- Low cost.
- Easy to use.
- It can also penetrate through walls.
- It creates an adhoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has slow data transfer rate: 3 Mbps.
- It has small range: 10 meters.